STIC EIC 2100 Search Request Form

116237

38

Today's Date:	What date would you like to use to limit the search?	
March 8, 2004	Priority Date: 1/7/98	Other:

Name Michael Simitoski AU 2134 Examiner # 79943 Room # PK2-5R03a Phone 703-305-8191 Serial # 09/764,794	**Format for Search Results (Circle One):** PAPER DISK EMAIL **Where have you searched so far?** USP DWPI EPO JPO ACM IBM TDB IEEE INSPEC SPI Other _____

Is this a "Fast & Focused" Search Request? (Circle One) YES NO

A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

I'm looking at claim 37. There is a very specific layout for cryptographic transmission where two devices exchange a message (originator and receiver), where the originator derives a first key from 3 pieces of data: a base key (shared), a first data string and data specific to the message (possibly a hash), a second key based on 3 things: the shared base key, a second string and the same data specific to the message -- where the originator hashes the message with the first key to get a signature and encrypts the signature and the message with the second key to obtain an "encrypted message" and joins (presumably concatenates) the "encrypted message" with the data specific to the message (once again, probably a has).

Specifically, I can't find

1. having a first and second key, both derived from the specifics of the claim.
2. hashing the message with the first key and encrypting the hashed message (signature) and the original message with the second key (although with art on the key derivation above, I probably could make a rejection). Hashing (keyed and non-keyed) is well known, as are messages with attached digital signatures (the combination encrypted or in the clear).

Terms:
Data specific to the message = hash, digest, signature, fingerprint, checksum, even an ID number
base key = shared key, private key, local key
first and second data strings can be just about anything

STIC Searcher Terese Esterhold	Phone 308-7795
Date picked up 3/9/04 4:15pm	Date Completed 3/10/04 5:00pm

Search and Information Resources Administration

```
Set     Items   Description
S1         77   AU=(TUNIMAN, D? OR TUNIMAN D? OR GOLDSCHMIDT, P? OR GOLDSC-
               HMIDT P? OR O'LEARY, M? OR O'LEARY M? OR KADYK, D? OR KADYK D-
               ?)
S2         30   S1 AND IC=H04L?
File 347:JAPIO Oct 1976-2003/Oct(Updated 040202)
         (c) 2004 JPO & JAPIO
File 348:EUROPEAN PATENTS 1978-2004/Feb W05
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040304,UT=20040226
         (c) 2004 WIPO/Univentio
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200416
         (c) 2004  THOMSON DERWENT
```

2/5/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01474591
Methods and systems for authentication through multiple proxy servers
Verfahren und Systeme zur Authentifizierung durch eine Vielzahl von Proxy-Servern
Procede et systemes pour l'authentification par l'intermediaire de plusieurs serveurs proxy
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
Kadyk, Donald J. , 20022 34th Avenue SE, Bothell, WA 98012, (US)
Fishman, Neil S., 23710 22nd Drive SE, Bothell, WA 98021, (US)
Damour, Kevin T., 4275 148th Avenue NE, Apt.F-203, Bellevue, WA 98007-8105, (US)
Kramer, Michael, 29 Fanshaw Avenue, Yonkers, New York 10705, (US
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1251672 A1 021023 (Basic)
APPLICATION (CC, No, Date): EP 2002008582 020416;
PRIORITY (CC, No, Date): US 838408 010419
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **H04L-029/06**

ABSTRACT EP 1251672 A1
Methods, systems, computer program products and data structures are described which allow a client to communicate with a server even though multiple proxies that require different authentication data must be traversed to allow such communication. In operation, the client first authenticates to a first proxy using authentication data appropriate for the first proxy. The client then authenticates to a second proxy using different authentication data that is appropriate for the second proxy. This proxy authentication continues through as many proxies as necessary until the client is in communication with the server.
ABSTRACT WORD COUNT: 92
NOTE:
Figure number on first page: 3

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 021023 A1 Published application with search report
Examination: 030122 A1 Date of request for examination: 20021126
Examination: 030903 A1 Date of dispatch of the first examination report: 20030718
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200243	1613
SPEC A	(English)	200243	6208
Total word count - document A			7821
Total word count - document B			0
Total word count - documents A + B			7821

2/5/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01474381
Negotiating secure connections through a proxy server
Verhandlung von sicheren Verbindungen durch einen Proxy-Server
Negociations de connexions securisees a travers d'un serveur proxy

PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
Kadyk, Donald J. , 20022 34th Avenue, SE, Bothell, WA 98028, (US)
Fishman, Neil S., 23710 22nd Drive, SE, Bothell, WA 98021, (US)
Seinfeld, Marc E., 16001 Inglewood Road, NE, Kenmore, WA 98028, (US)
Kramer, Michael, 29, Fanshaw Avenue, Yonkers, NY 10705, (US
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1251670 A2 021023 (Basic)
EP 1251670 A3 031210
APPLICATION (CC, No, Date): EP 2002007078 020327;
PRIORITY (CC, No, Date): US 838745 010419
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **H04L-029/06 ; H04L-029/08**

ABSTRACT EP 1251670 A2
Methods, systems, and computer program products for negotiating a secure end-to-end connection using a proxy server as an intermediary. The client first negotiates a secure connection between the client and the proxy so that any credentials exchanged will be encrypted. After the exchange of authentication credentials, the secure client-proxy connection is altered so that no further encryption takes place. The client and server then negotiate a secure end-to-end connection through the proxy, with the secure end-to-end connection being encapsulated within the insecure client-proxy connection. In this way, the overhead of creating a separate client-proxy connection for the secure end-to-end connection may be avoided, but the insecure client-proxy connection introduces only minimal overhead because it no longer encrypts any data that it carries.
ABSTRACT WORD COUNT: 123
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 021023 A2 Published application without search report
Change: 031210 A2 International Patent Classification changed: 20031024
Search Report: 031210 A3 Separate publication of the search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200243	843
SPEC A	(English)	200243	7471
Total word count - document A			8314
Total word count - document B			0
Total word count - documents A + B			8314

2/5/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01440046
Caching transformed content in a mobile gateway
Zwischenspeicherung von transformierten Inhaltsdaten in einem mobilen Gateway
Antememorisation de donneis transformeis dans une passerelle mobile
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
Fishman, Neil, 23710 22nd Dr. SE, Bothell, WA 98012, (US)

Kadyk, Don , 20022 34th Avenue SE, Bothell, WA 98012, (US)
Curtis, Brent, 23 Fulton Street, Seattle, WA 98109, (US)
Seinfeld, Marc, 16001 Inglewood Road NE, Kenmore, WA 98028, (US)
Ledsome, Mark, 2364 Fairview Avenue, East, Apt. 10, Seattle, WA 98102, (US
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1227637 A2 020731 (Basic)
APPLICATION (CC, No, Date): EP 2002001452 020121;
PRIORITY (CC, No, Date): US 771184 010126
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **H04L-029/06 ; H04L-012/66**

ABSTRACT EP 1227637 A2
A mobile gateway receives content from a content source and customizes the content using transforms assigned to each mobile client. Transforms account for differences between mobile clients without imposing significant processing burdens on the content server. Copies of the content, the transformed content, and a transform identifier are cached at the mobile gateway so that subsequent requests for the content may be satisfied without requiring access to the content source. Processing that is common among several transforms may be shared. Mobile clients may be any type of computer.
ABSTRACT WORD COUNT: 89
NOTE:
Figure number on first page: 2

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020731 A2 Published application without search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200231	2266
SPEC A	(English)	200231	7119
Total word count - document A			9385
Total word count - document B			0
Total word count - documents A + B			9385

2/5/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01439960
Establishing a secure connection with a private corporate network over a public network
Herstellung einer gesicherten Verbindung mit einem privaten Unternehmensnetz uber ein offentliches Netz
Etablissement d'une connection securisee avec un reseau d'entreprise prive passant par un reseau public
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
Kramer, Michael, 29 Fanshaw Avenue, Yonkers, New York 10705, (US)
Kadyk, Donald J. , 20022 34th Avenue SE, Bothell, Washington 98012, (US)
Fishman, Neil S., 23710 22nd Drive SE, Bothell, Washington 98012, (US
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1227634 A2 020731 (Basic)
EP 1227634 A3 020918
APPLICATION (CC, No, Date): EP 2002000904 020115;
PRIORITY (CC, No, Date): US 768673 010124

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **H04L-029/06**

ABSTRACT EP 1227634 A2
An external client securely accesses a private corporate network using a communications device, but without the communications device being required to communicate through the private corporate network when communicating with resources external to the private corporate network. The external client establishes a connection with the private corporate network over the public network such as the Internet using, for example, Transmission Control Protocol (TCP). The external client then provides security to the connection by running, for example, the Secure Socket Layer (SSL) protocol over the TCP protocol. During the ensuing session with the private corporate network, the communications device establishes a subsequent connection(s) with the external resource.
ABSTRACT WORD COUNT: 107
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020731 A2 Published application without search report
Search Report: 020918 A3 Separate publication of the search report
Examination: 021218 A2 Date of request for examination: 20021018
Examination: 030108 A2 Date of dispatch of the first examination report: 20021120
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200231	1430
SPEC A	(English)	200231	4689
Total word count - document A			6119
Total word count - document B			0
Total word count - documents A + B			6119

2/5/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01439956
A method, system and computer program product for synchronizing data represented by different data structures by using update notifications
Verfahren, System and Computerprogrammprodukt fur die Synchronisation von verschiedenen Datenstrukturen durch Benutzung von Aktualisierungsmeldungen
Procede, systeme et logiciel pour la synchronisation de differentes structures de donnees en utilisant des notifications d'actualisation
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
Kadyk, Donald J. , 20022 34th, Avenue SE, Bothell, Washington 98012, (US)
Fishman, Neil S., 23710 22nd Drive SE, Bothell, Washington 98021, (US)
Seinfield, Marc E., 16001 Inglewood Road NE, Kenmore, Washington 98028, (US
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1227396 A1 020731 (Basic)
APPLICATION (CC, No, Date): EP 2002000878 020115;
PRIORITY (CC, No, Date): US 768747 010124
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: G06F-009/445; G06F-009/44; H04L-029/06

ABSTRACT EP 1227396 A1

Methods, systems, and computer program products for synchronizing data (282) stored at one or more message clients (260) with data (220) stored at a message server (210) where the message clients may receive update notifications (290) and may represent the data using different data structures than the message server uses to represent the same data. A token (294) is associated with each data change that occurs at the message server. The message server sends each change and associated token to the message clients. When the message clients request a synchronization, the tokens they received are returned to the message server for comparison with the tokens the message server sent to the message clients. If the message clients do not return a particular token, the message server determines that the clients did not receive the corresponding change and resends the change to the message clients. Tokens may also be used to divide a change into one or more portions, with only one portion being provided initially. Then, in response to receiving the token associated with the portion, the message server may provide the remaining portion of the message to the message clients.

ABSTRACT WORD COUNT: 192

NOTE:
Figure number on first page: 2

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020731 A1 Published application with search report
Examination: 021023 A1 Date of request for examination: 20020821
Examination: 030115 A1 Date of dispatch of the first examination report: 20021127

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200231	2364
SPEC A	(English)	200231	6784
Total word count - document A			9148
Total word count - document B			0
Total word count - documents A + B			9148

2/5/6 (Item 6 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01414684

Using an expert proxy server as an agent for wireless devices
Verwendung eines Expert-Proxy-Servers als Agent fur drahtlose Vorrichtungen
Utilisation d'un serveur proxy expert comme agent pour des dispositifs sans fil

PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)

INVENTOR:
Kadyk, Donald J. , 20022 34th Avenue SE, Bothell, WA 98012, (US)
Fishmann, Neil S., 23710 22nd Drive SE, Bothell, WA 98012, (US)
Seinfeld, Marc, 16001 Inglewood Road NE, Kenmore, WA 98029, (US

LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 1195949 A2 020410 (Basic)
APPLICATION (CC, No, Date): EP 2001123665 011002;
PRIORITY (CC, No, Date): US 684053 001006
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **H04L-012/28** ; **H04L-029/06**

ABSTRACT EP 1195949 A2

An expert proxy server is described that is coupled to a number of wireless devices through a wireless network, and to a number of server computer systems through an external network such as, for example, the Internet. The expert proxy server acts as an agent for a wireless device by providing a service for the wireless device. Specifically, the expert proxy server determines that a service is to be provided to the wireless device. Next, the expert proxy server identifies an application that provides the service and then communicates with the identified application that provides the service. The expert proxy server compiles the results of the communication with the application and then transmits the compilation to the wireless device over the wireless network. Thus, the relatively smaller bandwidth of the wireless network is preserved by transmitting a minimal amount of information over the wireless network while leaving more extensive communications to occur over higher bandwidth external networks. Also, since the extensive processing occurs at the expert proxy server rather than at the wireless device, the application on the wireless device may be simplified and smaller as compared to the supporting applications on the expert proxy server thereby preserving the limited memory and processing capability of the wireless device.

ABSTRACT WORD COUNT: 209

NOTE:

Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application: 020410 A2 Published application without search report

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200215	1434
SPEC A	(English)	200215	5244
Total word count - document A			6678
Total word count - document B			0
Total word count - documents A + B			6678

2/5/7 (Item 7 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01265019

A flexible system and method for communicating between a broad range of networks and devices

Flexible System und Verfahren zur Kommunikation zwischen verschiedenen Netzwerken und Vorrichtungen

Systeme et procede souple pour la communication parmi des reseaux et dispositifs tres divers

PATENT ASSIGNEE:

MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)

INVENTOR:

Kadyk, Donald J. , 20022 34th Avenue SE, Bothell, WA 98012, (US)

Pederson, Leif, 13802 217th Place NE, Woodenville, WA 98072, (US)

Fishman, Neil S., 23710 22nd Dr. SE, Bothwell, WA 98012, (US)

Seinfeld, Marc E., 16001 Inglewood Road NE, Kenmore, WA 98028, (US

LEGAL REPRESENTATIVE:

Belcher, Simon James (58311), Urquhart-Dykes & Lord Tower House Merrion Way, Leeds LS2 8PA, (GB)

PATENT (CC, No, Kind, Date): EP 1091532 A2 010411 (Basic)
EP 1091532 A3 040107

APPLICATION (CC, No, Date): EP 2000308747 001004;

PRIORITY (CC, No, Date): US 411594 991004

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: **H04L-029/06** ; **H04L-012/58**

ABSTRACT EP 1091532 A2

A flexible gateway accommodates data transfer from a data origination device over a wide variety of networks to a wide variety of destination devices, even if those networks use different protocols, and even if the devices recognize different data formats. Thus, the gateway can perform work previously requiring numerous gateways. After the gateway receives information from a data source, the gateway identifies the specific device type and the specific network type to which the information is to be routed. The gateway then calls device and network drivers associated with the specific device and network identified with the destination device. These drivers then manipulate the data using the device driver into the format recognized by the destination device, and then provide the manipulated data to the destination device over the identified network using the compatible protocol. Thus, the destination device properly receives and interprets the information provided by the data source. If, in the very next moment, data arrives at the gateway that is to be routed over a different network using a different protocol to a different device recognizing a different device, the gateway will call different device and network drivers to enable the communication.

ABSTRACT WORD COUNT: 196

NOTE:

Figure number on first page: NONE

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	010411	A2 Published application without search report
Change:	040107	A2 International Patent Classification changed: 20031119
Search Report:	040107	A3 Separate publication of the search report

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200115	2042
SPEC A	(English)	200115	8404
Total word count - document A			10446
Total word count - document B			0
Total word count - documents A + B			10446

2/5/8 (Item 8 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01265018

Methods and systems for conversion of data format

Verfahren und Systemen zur Konvertierung von Datenformaten

Procedees et systemes pour la conversion du format des donnees

PATENT ASSIGNEE:

MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)

INVENTOR:

Kadyk, Donald , 20022 34th Avenue SE, Bothell, WA 98012, (US)

Fishman, Neil, 23710 22nd Dr SE, Bothell, WA 98012, (US)

Seinfeld, Marc, 16001 Inglewood Road NE, Kenomore, WA 98028, (US

LEGAL REPRESENTATIVE:

Belcher, Simon James (58311), Urquhart-Dykes & Lord Tower House Merrion Way, Leeds LS2 8PA, (GB)

PATENT (CC, No, Kind, Date): EP 1091536 A2 010411 (Basic)
EP 1091536 A3 031217

APPLICATION (CC, No, Date): EP 2000308746 001004;

PRIORITY (CC, No, Date): US 411594 991004; US 609269 000630

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: **H04L-029/06**

ABSTRACT EP 1091536 A2

The dynamic conversion of a data structure from an origin data format

into a destination data format is described. Instead of using a single data conversion module to accomplish this data conversion, a gateway computer system identifies a sequence of format conversion modules that, when executed in sequence, converts the data structure from the origin to the destination data format. The conversion occurs dynamically during run time and reduces the amount of needed data conversion modules significantly, particularly when there is a large amount of possible origin data formats and destination data formats. This conversion is particularly useful when communicating over wireless networks since there is little standardization in wireless devices resulting in wireless devices having many different proprietary data formats.
ABSTRACT WORD COUNT: 122
NOTE:
Figure number on first page: NONE

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 010411 A2 Published application without search report
Search Report: 031217 A3 Separate publication of the search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200115	1236
SPEC A	(English)	200115	7651
Total word count - document A			8887
Total word count - document B			0
Total word count - documents A + B			8887

2/5/9 (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01168946
METHOD AND APPARATUS FOR PERFORMING ERROR CORRECTION BY COMBINING TWO INSTANCES OF A MESSAGE
VERFAHREN UND VORRICHTUNG ZUR AUSFUHRUNG VON FEHLERKORREKTUR DURCH KOMBINATION VON ZWEI INSTANZEN EINER NACHRICHT
PROCEDE ET APPAREIL DE CORRECTION D'ERREUR PAR COMBINAISON DE DEUX INSTANCES D'UN MESSAGE
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749861), One Microsoft Way, Redmond, Washington 98052-6399, (US), (Applicant designated States: all)
INVENTOR:
KADYK, Don , 20022 - 34th Avenue S.E., Bothell, WA 98012, (US)
DEO, Vinay, 16732 N.E. 35th Street, Bellevue, WA 98008, (US)
O'LEARY, Michael, J., 22823 N.E. 54th Street, Redmond, WA 98053, (US
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1129539 A1 010905 (Basic)
WO 200028693 000518
APPLICATION (CC, No, Date): EP 99962717 991109; WO 99US26393 991109
PRIORITY (CC, No, Date): US 188755 981109
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS: **H04L-001/08**
NOTE:
No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 000712 A1 International application. (Art. 158(1))
Application: 000712 A1 International application entering European phase
Application: 010905 A1 Published application with search report
Examination: 010905 A1 Date of request for examination: 20010608
LANGUAGE (Publication,Procedural,Application): English; English; English

2/5/10 (Item 10 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01071467
SYSTEM FOR TRANSMITTING SUBSCRIPTION INFORMATION AND CONTENT TO A MOBILE DEVICE
SYSTEM ZUR UBERTRAGUNG VON ZUGRIFFINFORMATIONEN UND WEB-INHALT ZU EINEM MOBILEN GERAT
SYSTEME PERMETTANT DE TRANSMETTRE DES INFORMATIONS ET UN CONTENU D'ABONNEMENT A UN DISPOSITIF MOBILE
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749861), One Microsoft Way, Redmond, Washington 98052-6399, (US), (Applicant designated States: all)
INVENTOR:
DEO, Vinay, 16732 N.E. 35th Street, Bellevue, WA 98008, (US)
TUNIMAN, David , 23044 N.E. 61st Street, Redmond, WA 98052, (US)
SIMON, Daniel, R., Apartment E227, 16340 N.E. 83rd Street, Redmond, WA 98052, (US
LEGAL REPRESENTATIVE:
McLeish, Nicholas Alistair Maxwell et al (74621), Boult Wade Tennant Verulam Gardens 70 Gray's Inn Road, London WC1X 8BT, (GB)
PATENT (CC, No, Kind, Date): EP 1051824 A1 001115 (Basic)
WO 9935801 990715
APPLICATION (CC, No, Date): EP 99904038 990107; WO 99US309 990107
PRIORITY (CC, No, Date): US 70720 980107; US 74236 980210; US 75123 980213; US 108145 980630
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: **H04L-029/06** ; **H04L-012/28**
CITED PATENTS (WO A): WO 9728649 A ; WO 9512931 A
NOTE:
No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 001115 A1 Published application with search report
Application: 990915 A1 International application. (Art. 158(1))
Examination: 001115 A1 Date of request for examination: 20000710
Application: 990915 A1 International application entering European phase
LANGUAGE (Publication,Procedural,Application): English; English; English

2/5/11 (Item 11 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01071276
LOW LEVEL CONTENT FILTERING
INHALTSFILTERUNG AUF NIEDRIGEM NIVEAU
FILTRAGE DE CONTENU BAS NIVEAU
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749861), One Microsoft Way, Redmond, Washington 98052-6399, (US), (Applicant designated States: all)
INVENTOR:
KADYK, Don , 20022, 34th Avenue, SE, Bothell, WA 98012, (US)
O'LEARY, Michael, J., 22823 N.E. 54th Street, Redmond, WA 98053, (US)
CRONIN, Dennis, 2428 159th Avenue N.E., Bellevue, WA 98008, (US
LEGAL REPRESENTATIVE:
McLeish, Nicholas Alistair Maxwell et al (74621), Boult Wade Tennant Verulam Gardens 70 Gray's Inn Road, London WC1X 8BT, (GB)
PATENT (CC, No, Kind, Date): EP 1060597 A2 001220 (Basic)
WO 9935778 990715
APPLICATION (CC, No, Date): EP 99901360 990107; WO 99US337 990107
PRIORITY (CC, No, Date): US 70720 980107; US 75123 980213; US 107724 980630 ; US 107666 980630; US 189591 981110
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: **H04L-012/56** ; H04Q-007/14
CITED PATENTS (WO A): Y Y A A A

NOTE:
No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 001220 A2 Published application without search report
Application: 990915 A1 International application. (Art. 158(1))
Change: 010321 A2 Inventor information changed: 20010127
Examination: 001220 A2 Date of request for examination: 20000804
Application: 990915 A1 International application entering European phase
LANGUAGE (Publication,Procedural,Application): English; English; English

2/5/12 (Item 12 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01071275
SYSTEM FOR DELIVERING DATA CONTENT OVER A LOW BIT RATE TRANSMISSION CHANNEL
SYSTEM ZUR AUFGABE VON DATEN UBER EINEN NIEDRIGEN BITRATEN-UBERTRAGUNGSKANAL
SYSTEME PERMETTANT D'ENVOYER UN CONTENU DE DONNEES SUR UN CANAL DE TRANSMISSION A FAIBLE DEBIT BINAIRE
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749861), One Microsoft Way, Redmond, Washington 98052-6399, (US), (Applicant designated States: all)
INVENTOR:
WECKER, Dave, 23908 - 22nd Drive, S.E., Bothell, WA 98021, (US)
DEO, Vinay, 16732 N.E. 35th Street, Bellevue, WA 98008, (US)
MILLER, John, Mark, 8026 N.E. 122nd Place, Kirkland, WA 98034, (US)
TUNIMAN, David , 23044 N.E. 61st Street, Redmond, WA 98053, (US)
O'LEARY, Michael, J., 22823 N.E. 54th Street, Redmond, WA 98053, (US
LEGAL REPRESENTATIVE:
McLeish, Nicholas Alistair Maxwell et al (74621), Boult Wade Tennant Verulam Gardens 70 Gray's Inn Road, London WC1X 8BT, (GB)
PATENT (CC, No, Kind, Date): EP 1051823 A1 001115 (Basic)
WO 9935802 990715
APPLICATION (CC, No, Date): EP 99901359 990107; WO 99US336 990107
PRIORITY (CC, No, Date): US 70720 980107; US 75123 980213; US 107666 980630
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: **H04L-029/06**
CITED PATENTS (WO A): XP 2016896 ; XP 4095309
CITED REFERENCES (WO A):
KAASHOEK M F ET AL: "DYNAMIC DOCUMENTS: MOBILE WIRELESS ACCESS TO THE WWW" PROCEEDINGS, WORKSHOP ON MOBILE COMPUTING SYSTEMS AND APPLICATIONS,8 December 1994, pages 179-184, XP002016896
VITALI F ET AL: "Extending HTML in a principled way with displets" COMPUTER NETWORKS AND ISDN SYSTEMS, vol. 29, no. 8-13, 1 September 1997, page 1115-1128 XP004095309;
NOTE:
No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 001115 A1 Published application with search report
Application: 990915 A2 International application. (Art. 158(1))
Examination: 001115 A1 Date of request for examination: 20000707
Application: 990915 A2 International application entering European phase
LANGUAGE (Publication,Procedural,Application): English; English; English

2/5/13 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00565320 **Image available**
METHOD AND APPARATUS FOR PERFORMING ERROR CORRECTION BY COMBINING TWO INSTANCES OF A MESSAGE
PROCEDE ET APPAREIL DE CORRECTION D'ERREUR PAR COMBINAISON DE DEUX

INSTANCES D'UN MESSAGE
Patent Applicant/Assignee:
MICROSOFT CORPORATION,
Inventor(s):
KADYK Don ,
DEO Vinay,
O'LEARY Michael J
Patent and Priority Information (Country, Number, Date):
Patent: WO 200028693 A1 20000518 (WO 0028693)
Application: WO 99US26393 19991109 (PCT/WO US9926393)
Priority Application: US 98188755 19981109
Designated States: CA JP AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-001/08**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 8832

English Abstract
First and second instances (264, 266) of a message are received over a wireless connection (202, 204). It is determined whether the first and second instances (264, 266) of the message contain an error. If both instances contain an error, an error free instance (264) of the message is reconstructed from the two erroneous instances by merging portions of the first and second instances (264, 266).

French Abstract
Les premiere et seconde instances (264, 266) d'un message sont recues sur une connexion sans fil (202, 204). On determine si ces premiere et secondes instances (264, 266) du message contiennent une erreur. Si les deux instances contiennent une erreur, une instance (264) du message sans erreur est reconstruite a partir des deux instances erronees par fusion de parties des premiere et seconde instances (264, 266).

2/5/14 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00504450 **Image available**
SYSTEM FOR DELIVERING DATA CONTENT OVER A LOW BIT RATE TRANSMISSION CHANNEL
SYSTEME PERMETTANT D'ENVOYER UN CONTENU DE DONNEES SUR UN CANAL DE TRANSMISSION A FAIBLE DEBIT BINAIRE
Patent Applicant/Assignee:
MICROSOFT CORPORATION,
Inventor(s):
WECKER Dave,
DEO Vinay,
MILLER John Mark,
TUNIMAN David ,
O'LEARY Michael J
Patent and Priority Information (Country, Number, Date):
Patent: WO 9935802 A1 19990715
Application: WO 99US336 19990107 (PCT/WO US9900336)
Priority Application: US 9870720 19980107; US 9875123 19980213; US 98107666 19980630
Designated States: CA JP AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-029/06**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 14770

English Abstract

The present invention provides a system by which information content (250) is delivered to a mobile device (18). The web content (250) is divided into data (202) and script information (204). The script information (204) is used to operate on the data (202) to render the data (202) in a predetermined format.

French Abstract

Cette invention a trait a un systeme permettant d'envoyer un contenu d'information (250) a un dispositif mobile (18). Le contenu du lacis (250) est divise en donnees (202) et information de script (204). On utilise cette information de script (204) pour prendre en charge les donnees (202) afin de les convertir a un format predetermine.

2/5/15 (Item 3 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

00504449 **Image available**

SYSTEM FOR TRANSMITTING SUBSCRIPTION INFORMATION AND CONTENT TO A MOBILE DEVICE

SYSTEME PERMETTANT DE TRANSMETTRE DES INFORMATIONS ET UN CONTENU D'ABONNEMENT A UN DISPOSITIF MOBILE

Patent Applicant/Assignee:
MICROSOFT CORPORATION,
Inventor(s):
DEO Vinay,
TUNIMAN David ,
SIMON Daniel R

Patent and Priority Information (Country, Number, Date):
Patent: WO 9935801 A1 19990715
Application: WO 99US309 19990107 (PCT/WO US9900309)
Priority Application: US 9870720 19980107; US 9874236 19980210; US 9875123 19980213; US 98108145 19980630
Designated States: CA JP AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-029/06**
International Patent Class: **H04L-012/28**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 16525

English Abstract

A system controls access to broadcast messages (298) received by a plurality of mobile devices (18). Selected mobile devices (18) are provided with a broadcast encryption key (BEK) (268). The broadcast messages (298) are encrypted using the BEK (268) prior to broadcasting so that the selected mobile devices (18) containing the BEK (268) can decrypt the broadcast messages (298). The broadcast messages (298) are then broadcast.

French Abstract

L'invention concerne un systeme qui permet de commander l'acces a des messages a diffusion generale (298) recus par une pluralite de dispositifs mobiles (18). Des dispositifs mobiles (18) selectionnes comportent une cle de cryptage de diffusion (BEK) (268). Les messages diffuses (298) sont cryptes a l'aide de la cle de cryptage (268) avant leur diffusion, de facon a pouvoir etre decryptes par les dispositifs mobiles (18) selectionnes contenant ladite cle (268). Puis les messages sont diffuses.

2/5/16 (Item 4 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

00504426 **Image available**
LOW LEVEL CONTENT FILTERING
FILTRAGE DE CONTENU BAS NIVEAU
Patent Applicant/Assignee:
MICROSOFT CORPORATION,
Inventor(s):
KADYK Don ,
O'LEARY Michael J,
CRONIN Dennis
Patent and Priority Information (Country, Number, Date):
Patent: WO 9935778 A2 19990715
Application: WO 99US337 19990107 (PCT/WO US9900337)
Priority Application: US 9870720 19980107; US 9875123 19980213; US 98107724 19980630; US 98107666 19980630; US 98189591 19981110
Designated States: CA JP AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-012/56**
International Patent Class: H04Q-007/14
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 16617

English Abstract
A system and method for receiving wireless information on a portable device (10) includes receiving an information packet (160) comprising a first portion having topic information (166) indicative of content in the second portion (170) of the information packet (160). The first portion of the information packet (160) is compared to content filter data (206) stored on the portable computing device (10). At least the second portion (170) of the information packet is forwarded to another component of the portable computing device if the first portion matches any of the content filter data (206).

French Abstract
Cette invention a trait a un systeme ainsi qu'a la technique correspondante permettant de recevoir une information radio sur un appareil portable (10), laquelle technique consiste a recevoir un paquet d'informations (160) comportant une premiere partie renfermant une information de sujet (166) representative d'un contenu de la seconde partie (170) du paquet d'informations (160). La premiere partie du paquet d'informations (160) est comparee a des donnees de filtre de contenu (206) memorisees dans le dispositif de calcul portable (10). La seconde partie au moins (170) du paquet d'informations est expediee a un autre composant du dispositif de calcul portable si la premiere partie est en concordance avec les donnees de filtre de contenu (206), quelles qu'elles soient.

2/5/17 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00504239 **Image available**
A SYSTEM FOR PROGRAMMING A MOBILE DEVICE IN A PROTOCOL, DEVICE, AND NETWORK INDEPENDENT FASHION
SYSTEME PERMETTANT UNE DIFFUSION VERS UN DISPOSITIF MOBILE ET LA PROGRAMMATION DE CELUI-CI DE MANIERE INDEPENDANTE DU PROTOCOLE, DU DISPOSITIF ET DU RESEAU
Patent Applicant/Assignee:
MICROSOFT CORPORATION,
Inventor(s):
DEO Vinay,
TUNIMAN David ,

GOLDSCHMIDT Pamela ,
O'LEARY Michael J,
KADYK Don
Patent and Priority Information (Country, Number, Date):
Patent: WO 9935591 A2 19990715
Application: WO 99US325 19990107 (PCT/WO US9900325)
Priority Application: US 9870720 19980107; US 9874236 19980210; US 9875123 19980213; US 98108953 19980630
Designated States: CA JP AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-012/28**
International Patent Class: H04Q-007/12; **H04L-029/06 ; H04L-009/32 ; H04L-009/08**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 15255

English Abstract
The present invention is directed, in one embodiment, to a programming interface which enables device/protocol/network independent transmission of messages to, and programming of, mobile devices (18). In another embodiment, the present invention is directed to data structures maintained on, and supported by, the mobile devices (18). The present invention also, in another embodiment, provides security for programming messages and an acknowlegement channel over which the mobile device (18) can acknowledge receipt of, and successful implementation of, a programming message (288).

French Abstract
Cette invention a trait, dans un mode de realisation, a une interface de programmation permettant de transmettre des messages a un dispositif mobile (18) et de le programmer de maniere independante du dispositif, du protocole et du reseau. Dans un autre mode de realisation, cette invention porte sur des structures de donnees conservees et prises en charge par les dispositifs mobiles (18). Dans un autre mode de realisation elle porte egalement sur la securite de messages de programmation ainsi que sur un canal d'accuse de reception sur lequel le dispositif mobile (18) peut accuser reception d'un message de programmation (288) et du succes de sa mise en oeuvre .

2/5/18 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015061977 **Image available**
WPI Acc No: 2003-122493/200312
XRPX Acc No: N03-097524
Electronic authentication method for computer network, involves authenticating primary and secondary proxy computers for establishing communication between client and server computers
Patent Assignee: MICROSOFT CORP (MICT); DAMOUR K T (DAMO-I); FISHMAN N S (FISH-I); KADYK D J (KADY-I); KRAMER M (KRAM-I)
Inventor: DAMOUR K T; FISHMAN N S; **KADYK D J** ; KRAMER M
Number of Countries: 027 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1251672	A1	20021023	EP 20028582	A	20020416	200312	B
US 20020156906	A1	20021024	US 2001838408	A	20010419	200312	

Priority Applications (No Type Date): US 2001838408 A 20010419
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1251672	A1	E	23	H04L-029/06	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT

LI LT LU LV MC MK NL PT RO SE SI TR
US 20020156906 A1 G06F-015/16

Abstract (Basic): EP 1251672 A1

NOVELTY - A request for a service is dispatched by a client computer (201). The primary and the secondary proxy computers (202,204) are authenticated using the authentication data and the communication between the client computer and the server computer (201) is established.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for computer readable medium storing network communication program.

USE - For computer network.

ADVANTAGE - Maintains a high degree of confidentiality between the multiple proxies, without changing the existing standards, by authenticating the proxy computers.

DESCRIPTION OF DRAWING(S) - The figure shows an explanatory view of computer network.

Client computer (201)

Proxy computers (202,204)

pp; 23 DwgNo 3/11

Title Terms: ELECTRONIC; AUTHENTICITY; METHOD; COMPUTER; NETWORK; AUTHENTICITY; PRIMARY; SECONDARY; COMPUTER; ESTABLISH; COMMUNICATE; CLIENT; SERVE; COMPUTER

Derwent Class: T01

International Patent Class (Main): G06F-015/16; **H04L-029/06**

File Segment: EPI

2/5/19 (Item 2 from file: 350)

DIALOG(R)File 350:Derwent WPIX

015061975 **Image available**

WPI Acc No: 2003-122491/200312

XRPX Acc No: N03-097522

Secure connection negotiation method through proxy system, involves negotiating secure client-proxy and client-server connections, and encapsulating client-server connection within insecure client-proxy connection

Patent Assignee: MICROSOFT CORP (MICT); FISHMAN N S (FISH-I); KADYK D J (KADY-I); KRAMER M (KRAM-I); SEINFELD M E (SEIN-I)

Inventor: FISHMAN N S; **KADYK D J** ; KRAMER M; SEINEELD M E

Number of Countries: 027 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1251670	A2	20021023	EP 20027078	A	20020327	200312	B
US 20020157019	A1	20021024	US 2001838745	A	20010419	200312	

Priority Applications (No Type Date): US 2001838745 A 20010419

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1251670	A2	E	20	H04L-029/06	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

US 20020157019 A1 H04L-009/00

Abstract (Basic): EP 1251670 A2

NOVELTY - A secure connection between a client system and a proxy system is negotiated. A secure end-to-end connection is negotiated between the client and a server system using the client-proxy connection, and then the client-proxy connection is altered to be insecure. The secure end-to-end connection is encapsulated with the insecure client-proxy connection.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for computer program product comprising recorded medium storing secure connection negotiation program.

USE - For negotiating secure connection through proxy system of

computer network.

ADVANTAGE - Provides a secure client-server connection that is linked through a proxy, capable of exchanging encrypted data between the client and server. Minimizes communication overhead between client and server, as the data carried by client-proxy connection is not encrypted or decrypted.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the secure client-sever connection negotiation system.

pp; 20 DwgNo 1/5

Title Terms: SECURE; CONNECT; NEGOTIATE; METHOD; THROUGH; SYSTEM; NEGOTIATE ; SECURE; CLIENT; CLIENT; SERVE; CONNECT; ENCAPSULATE; CLIENT; SERVE; CONNECT; CLIENT; CONNECT

Derwent Class: T01

International Patent Class (Main): **H04L-009/00 ; H04L-029/06**

File Segment: EPI

2/5/20 (Item 3 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014891667 **Image available**

WPI Acc No: 2002-712373/200277

XRPX Acc No: N02-561924

Online secure connection establishment method for private corporate network, involves retaining ability of external client to establish separate and distinct connection with external resources outside the network

Patent Assignee: MICROSOFT CORP (MICT); FISHMAN N S (FISH-I); KADYK D J (KADY-I); KRAMER M (KRAM-I)

Inventor: FISHMAN N S; **KADYK D J ;** KRAMER M

Number of Countries: 027 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020099957	A1	20020725	US 2001768673	A	20010124	200277	B
EP 1227634	A2	20020731	EP 2002904	A	20020115	200277	

Priority Applications (No Type Date): US 2001768673 A 20010124

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020099957	A1		12	H04L-009/00	
EP 1227634	A2	E		H04L-029/06	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

Abstract (Basic): US 20020099957 A1

NOVELTY - An external client (340) establishes a secured connection with private corporate network (310) using secured socket layer (SSL) protocol. The client retains the ability to establish a separate and distinct connection with external resources (330a,330b) outside the network, while maintaining a session with the network.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for computer program product for establishing online secure connection over private corporate network.

USE - For establishing secure connection between external client and private corporate network over public network e.g internet.

ADVANTAGE - Since the ability of the external client to establish connection with external resources outside the private corporate network are retained, the external client is allowed to directly communicate with the external resource rather than through channel communications to external resource through the corporate network. Improves routing efficiency and security of the private corporate network.

DESCRIPTION OF DRAWING(S) - The figure shows a suitable network architecture for implementing the secure connection establishment method.

Private corporate network (310)

External resources (330a,330b)
External client (340)
pp; 12 DwgNo 3/4
Title Terms: SECURE; CONNECT; ESTABLISH; METHOD; PRIVATE; NETWORK; RETAIN; ABILITY; EXTERNAL; CLIENT; ESTABLISH; SEPARATE; DISTINCT; CONNECT; EXTERNAL; RESOURCE; NETWORK
Derwent Class: T01; W01
International Patent Class (Main): **H04L-009/00 ; H04L-029/06**
File Segment: EPI

2/5/21 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014885375 **Image available**
WPI Acc No: 2002-706081/200276
XRPX Acc No: N02-556662
Data synchronization method used in personal computer, handheld device, involves sending notification comprising change of data and token identifying change to receiving device
Patent Assignee: MICROSOFT CORP (MICT); FISHMAN N S (FISH-I); KADYK D J (KADY-I); SEINFIELD M E (SEIN-I)
Inventor: FISHMAN N S; **KADYK D J** ; SEINFIELD M E
Number of Countries: 027 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020099727	A1	20020725	US 2001768747	A	20010124	200276	B
EP 1227396	A1	20020731	EP 2002878	A	20020115	200276	

Priority Applications (No Type Date): US 2001768747 A 20010124
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020099727	A1		16	G06F-012/00	
EP 1227396	A1	E		G06F-009/445	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

Abstract (Basic): US 20020099727 A1
NOVELTY - The data (218) is changed and notification (290) comprising both the change (292) and a token (294) identifying the change is sent to a receiving device. A synchronization request is received from the device and the change is resend to the device if the request does not include the token.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:
(1) Data synchronization system; and
(2) Computer programmable product storing data synchronization instructions.
USE - Used in PC, handheld device, multi-processor system, microprocessor-based or programmable consumer electronics, network PC, minicomputer, mainframe computer, local and remote processing device for synchronizing data.
ADVANTAGE - The data is efficiently synchronized using the notification send to the receiving device and the notification can be updated without imposing burden on the user.
DESCRIPTION OF DRAWING(S) - The figure shows a block diagram of the data structures and communication channels for synchronizing client data with server data.
Data (218)
Notification (290)
Change (292)
Token (294)
pp; 16 DwgNo 2/4
Title Terms: DATA; SYNCHRONISATION; METHOD; PERSON; COMPUTER; DEVICE; SEND; NOTIFICATION; COMPRISE; CHANGE; DATA; TOKEN; IDENTIFY; CHANGE; RECEIVE; DEVICE

Derwent Class: T01; W01
International Patent Class (Main): G06F-009/445; G06F-012/00
International Patent Class (Additional): G06F-009/44; **H04L-029/06**
File Segment: EPI

2/5/22 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014780563 **Image available**
WPI Acc No: 2002-601269/200265
XRPX Acc No: N02-476639

Modified electronic content acquisition method for mobile client, involves applying transform considering mobile client operating characteristics to content received at mobile gateway

Patent Assignee: MICROSOFT CORP (MICT); CURTIS B (CURT-I); FISHMAN N (FISH-I); KADYK D (KADY-I); LEDSOME M (LEDS-I); SEINFELD M (SEIN-I)
Inventor: CURTIS B; FISHMAN N; **KADYK D** ; LEDSOME M; SEINFELD M
Number of Countries: 027 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1227637	A2	20020731	EP 20021452	A	20020121	200265	B
US 20020103934	A1	20020801	US 2001771184	A	20010126	200265	

Priority Applications (No Type Date): US 2001771184 A 20010126
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1227637	A2	E	22	H04L-029/06	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR					
US 20020103934	A1			G06F-015/16	

Abstract (Basic): EP 1227637 A2

NOVELTY - A transform specifically considering the operating characteristics of the mobile client is applied to the electronic content received at a mobile gateway (250). The transformed content is stored in a mobile gateway cache (280) and is returned to the mobile clients (274,276,278,279) in response to a request including transform identifier.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for computer program product storing transformed content obtaining program.

USE - For obtaining modified content such as e-mail content, web page content, financial data, sports information, notification, schedule, contact, configuration data which are transformed according to operating characteristics e.g. processor, memory, display, communication link, application or operating software of a mobile client e.g. telephone, pager, PDA, laptop, desktop, etc.

ADVANTAGE - A mobile gateway allows for support of new mobile clients without requiring modification to the content server. The added burdens of customizing content for mobile clients are met by the mobile gateway, without imposing significant processing overhead on the content server.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the mobile gateway for transforming e-mail content for mobile clients.

Mobile gateway (250)
Mobile gateway cache (280)
Mobile clients (274,276,278,279)
pp; 22 DwgNo 2/4

Title Terms: MODIFIED; ELECTRONIC; CONTENT; ACQUIRE; METHOD; MOBILE; CLIENT ; APPLY; TRANSFORM; MOBILE; CLIENT; OPERATE; CHARACTERISTIC; CONTENT; RECEIVE; MOBILE; GATEWAY
Derwent Class: T01; W01; W05
International Patent Class (Main): G06F-015/16; **H04L-029/06**
International Patent Class (Additional): **H04L-012/66**
File Segment: EPI

2/5/23 **(Item 6 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

014597995 **Image available**
WPI Acc No: 2002-418699/200245
XRPX Acc No: N02-329563

Agent service provision method in expert proxy server, involves compiling results of communication with application, for transmission to wireless device through wireless network

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: FISHMANN N S; **KADYK D J** ; SEINFELD M
Number of Countries: 026 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1195949	A2	20020410	EP 2001123665	A	20011002	200245	B

Priority Applications (No Type Date): US 2000684053 A 20001006
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1195949	A2	E	13	H04L-012/28	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

Abstract (Basic): EP 1195949 A2

NOVELTY - The expert proxy server (130) determines whether a service is to be provided to a wireless device, and identifies an application that provides the service. The expert proxy server compiles the results of the communication with the application, and then transmits the compilation to the wireless device (110) through wireless network (120).

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for computer program product for acting of expert proxy server as agent.

USE - In network environment for acting of expert proxy server connected to wireless devices, as agent.

ADVANTAGE - Since extensive processing occurs at the expert proxy server rather than at the wireless device, the application on the wireless device may be simplified and is smaller compared to the supporting applications on the expert proxy server, thereby preserving the limited memory and processing capability of the wireless device. During transmission, the smaller bandwidth of the wireless network is preserved by transmitting a minimal amount of information over the wireless network while leaving more extensive communications to occur over high bandwidth external networks.

DESCRIPTION OF DRAWING(S) - The figure shows a network environment.

Wireless device (110)
Wireless network (120)
Expert proxy server (130)
pp; 13 DwgNo 1/3

Title Terms: AGENT; SERVICE; PROVISION; METHOD; EXPERT; SERVE; COMPILE; RESULT; COMMUNICATE; APPLY; TRANSMISSION; WIRELESS; DEVICE; THROUGH; WIRELESS; NETWORK
Derwent Class: T01; W01
International Patent Class (Main): **H04L-012/28**
International Patent Class (Additional): **H04L-029/06**
File Segment: EPI

2/5/24 **(Item 7 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

014047062 **Image available**
WPI Acc No: 2001-531275/200159

Related WPI Acc No: 2001-531274
XRPX Acc No: N01-394495

Data format converting method in gate way computer system involves identifying sequence of conversion modules for converting data structure from primary data format to secondary data format

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: FISHMAN N; **KADYK D** ; SEINFELD M
Number of Countries: 025 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1091536	A2	20010411	EP 2000308746	A	20001004	200159	B

Priority Applications (No Type Date): US 2000609269 A 20000630; US 99411594 A 19991004
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1091536	A2	E	18	H04L-029/06	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Abstract (Basic): EP 1091536 A2

NOVELTY - The data structure is converted from primary data format into an intermediate data format using the primary format conversion module of identified sequence of data conversion modules. Then the data structure is converted from the intermediate data format into the secondary data format using the secondary format conversion module of the sequence.

DETAILED DESCRIPTION - The first data format is identified as received from the originating computer system. The second data format is identified as compatible with the remote computer systems. The remote computer system includes a server computer system or a wireless device. INDEPENDENT CLAIMS are also included for the following:

(a) Computer program product;

(b) Gate way computer system

USE - For converting data format in gate way computer system.

ADVANTAGE - Uses gate way computer system for both dynamic content translation and dynamic protocol and network translations. The conversion receives automatically upon the receipt of a given data structure without requiring any user intervention.

DESCRIPTION OF DRAWING(S) - The figure shows the data conversion system providing a suitable operating environment.

pp; 18 DwgNo 1/9

Title Terms: DATA; FORMAT; CONVERT; METHOD; GATE; WAY; COMPUTER; SYSTEM; IDENTIFY; SEQUENCE; CONVERT; MODULE; CONVERT; DATA; STRUCTURE; PRIMARY; DATA; FORMAT; SECONDARY; DATA; FORMAT
Derwent Class: W01
International Patent Class (Main): **H04L-029/06**
File Segment: EPI

2/5/25 (Item 8 from file: 350)

014047061 **Image available**
WPI Acc No: 2001-531274/200159
Related WPI Acc No: 2001-531275
XRPX Acc No: N01-394494

Computer program product for network computer system, has program codes to send message to destination device using protocol and identified format, irrespective of differences in originating and receiving protocols

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: FISHMAN N S; **KADYK D J** ; PEDERSON L; SEINFELD M E
Number of Countries: 026 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week

EP 1091532 A2 20010411 EP 2000308747 A 20001004 200159 B
US 6674767 B1 20040106 US 99411594 A 19991004 200411

Priority Applications (No Type Date): US 99411594 A 19991004
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
EP 1091532 A2 E 19 H04L-012/66
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI
US 6674767 B1 H04L-012/00

Abstract (Basic): EP 1091532 A2

NOVELTY - Message intended for remote destination device is received from originating device at gateway identified with device module associated with the intended remote destination device. Message is manipulated using device module and is then transmitted to destination device through network using protocol and recognized format, irrespective of differences in originating and receiving protocols.

DETAILED DESCRIPTION - A computer readable medium for providing computer program codes is utilized by the gateway to implement forwarding of data. One or more originating devices are logically connected to and communicate using one or more originating protocols with one or more originating networks logically connected to a gateway. Message generated at the originating device, that is intended for remote destination devices using receiving protocols. INDEPENDENT CLAIMS are also included for the following:

(a) Data communication method;

(b) Networked computer system

USE - Network computer system.

ADVANTAGE - Gateway accommodates data transfer from a data originating device over a wide variety of networks to a wide variety of destination devices even if those networks use different protocols and even if the devices recognize different data formats. The gateway is incorporated into wired as well as wireless networks, thus the gateway is beneficial in the wireless world where formats and protocols tend to vary device to device and network to network. The gateway is flexible as it facilitates both unidirectional and bidirection communication.

DESCRIPTION OF DRAWING(S) - The figure shows the networked computer system.

pp; 19 DwgNo 1/6

Title Terms: COMPUTER; PROGRAM; PRODUCT; NETWORK; COMPUTER; SYSTEM; PROGRAM ; CODE; SEND; MESSAGE; DESTINATION; DEVICE; PROTOCOL; IDENTIFY; FORMAT; IRRESPECTIVE; DIFFER; ORIGIN; RECEIVE
Derwent Class: W01
International Patent Class (Main): **H04L-012/00 ; H04L-012/66**
International Patent Class (Additional): **H04L-029/06**
File Segment: EPI

2/5/26 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 THOMSON DERWENT. All rts. reserv.

013250690 **Image available**
WPI Acc No: 2000-422573/200036
XRPX Acc No: N00-315372

Error message correction method for pager, involves reconstructing message by merging erroneous portions of instances to generate error-free message

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: DEO V; **KADYK D** ; O'LEARY M J
Number of Countries: 022 Number of Patents: 005
Patent Family:
Patent No Kind Date Applicat No Kind Date Week
WO 200028693 A1 20000518 WO 99US26393 A 19991109 200036 B
US 6209111 B1 20010327 US 98188755 A 19981109 200119

EP 1129539	A1	20010905	EP 99962717	A	19991109	200151	
			WO 99US26393	A	19991109		
JP 2002530008	W	20020910	WO 99US26393	A	19991109	200274	
			JP 2000581774	A	19991109		
US 6611937	B1	20030826	US 98188755	A	19981109	200357	
			US 2000692121	A	20001019		

Priority Applications (No Type Date): US 98188755 A 19981109; US 2000692121 A 20001019
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200028693	A1	E	53	H04L-001/08	
Designated States (National): CA JP					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
US 6209111	B1			G06F-011/00	
EP 1129539	A1	E		H04L-001/08	Based on patent WO 200028693
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
JP 2002530008	W		46	H04L-001/08	Based on patent WO 200028693
US 6611937	B1			G06F-011/00	Div ex application US 98188755 Div ex patent US 6209111

Abstract (Basic): WO 200028693 A1

NOVELTY - Instances of a message are received over a wireless connection. When the instances are judged to contain errors, the message is reconstructed, by merging erroneous portions of instances to generate error-free instances.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for data structure received by mobile device.

USE - For pager, handheld personal computer, palm PC.

ADVANTAGE - The correct contents of message is displayed to the user, by rectifying the errors reliably.

DESCRIPTION OF DRAWING(S) - The figure shows flowchart illustrating mobile device operation.

pp; 53 DwgNo 8/11

Title Terms: ERROR; MESSAGE; CORRECT; METHOD; PAGE; RECONSTRUCT; MESSAGE; MERGE; ERROR; PORTION; INSTANCE; GENERATE; ERROR; FREE; MESSAGE
Derwent Class: W01
International Patent Class (Main): G06F-011/00; **H04L-001/08**
International Patent Class (Additional): G06F-011/10; H03M-013/37; H04B-007/26; **H04L-001/00**
File Segment: EPI

2/5/27 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 THOMSON DERWENT. All rts. reserv.

012638168 **Image available**
WPI Acc No: 1999-444272/199937
Related WPI Acc No: 1999-419419; 1999-419431; 1999-419433; 1999-419451; 1999-444271; 2003-361578; 2003-419885
XRPX Acc No: N99-331350

Information content from content provider to mobile device providing system

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: DEO V; MILLER J M; O'LEARY M J; **TUNIMAN D** ; WECKER D
Number of Countries: 020 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9935802	A1	19990715	WO 99US336	A	19990107	199937	B
EP 1051823	A1	20001115	EP 99901359	A	19990107	200059	
			WO 99US336	A	19990107		
JP 2002501241	W	20020115	WO 99US336	A	19990107	200207	
			JP 2000528059	A	19990107		

Priority Applications (No Type Date): US 98107666 A 19980630; US 9870720 P 19980107; US 9875123 P 19980213
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
WO 9935802 A1 E 78 H04L-029/06
Designated States (National): CA JP
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
EP 1051823 A1 E H04L-029/06 Based on patent WO 9935802
Designated States (Regional): DE FR GB
JP 2002501241 W 76 G06F-013/00 Based on patent WO 9935802

Abstract (Basic): WO 9935802 A1
NOVELTY - A mobile device component is disposed on a mobile device and includes a receiver that receives the content from a transmitter. A router is coupled to the receiver and a second store to provide the script file and the data file to the second store. A transport is coupled to the second store and configured to selectively retrieve the data file and execute the script to place the data in the desired rendering form.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for: a computer program that includes instructions readable by a mobile device.
USE - In personal mobile computing devices commonly known as mobile devices for delivering and receiving information on a mobile device. The user of the mobile device may also have access to, and use, a desktop computer at work or at home, or both.
ADVANTAGE - Provides the ability to deliver content to a mobile device over a low bit rate channel in an economic and efficient manner. Small segments of data can be delivered instead of full HTML pages. The present invention also provides a mechanism by which logging and filtering can be accomplished in an efficient manner
DESCRIPTION OF DRAWING(S) - The drawing is a simplified block diagram illustrating one embodiment of a mobile device in a system in accordance with the principles of the present invention.
pp; 78 DwgNo 1/8
Title Terms: INFORMATION; CONTENT; CONTENT; MOBILE; DEVICE; SYSTEM
Derwent Class: T01; W01
International Patent Class (Main): G06F-013/00; **H04L-029/06**
International Patent Class (Additional): G06F-012/00; H04B-007/26; H04H-001/00
File Segment: EPI

2/5/28 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012638167 **Image available**
WPI Acc No: 1999-444271/199937
Related WPI Acc No: 1999-419419; 1999-419431; 1999-419433; 1999-419451; 1999-444272; 2003-361578; 2003-419885
XRPX Acc No: N99-331349
Access to broadcast messages received by number of mobile devices controlling
Patent Assignee: MICROSOFT CORP. (MICT)
Inventor: DEO V; SIMON D R; **TUNIMAN D**
Number of Countries: 021 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9935801	A1	19990715	WO 99US309	A	19990107	199937	B
EP 1051824	A1	20001115	EP 99904038	A	19990107	200059	
			WO 99US309	A	19990107		
JP 2002501334	W	20020115	WO 99US309	A	19990107	200207	
			JP 2000528058	A	19990107		
US 6496928	B1	20021217	US 9870720	P	19980107	200307	
			US 9874236	P	19980210		

US 9875123 P 19980213
US 98108145 A 19980630

Priority Applications (No Type Date): US 98108145 A 19980630; US 9870720 P 19980107; US 9874236 P 19980210; US 9875123 P 19980213
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9935801	A1	E	98	H04L-029/06	
Designated States (National): CA JP					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 1051824	A1	E		H04L-029/06	Based on patent WO 9935801
Designated States (Regional): DE FR GB					
JP 2002501334	W		109	H04L-009/08	Based on patent WO 9935801
US 6496928	B1			H04L-009/00	Provisional application US 9870720 Provisional application US 9874236 Provisional application US 9875123

Abstract (Basic): WO 9935801 A1
NOVELTY - The method involves providing selected mobile devices, of the number of mobile devices, with a broadcast encryption key (BEK) encrypting the broadcast messages utilizing the BEK prior to broadcasting the broadcast messages such that the selected mobile devices having the BEK are configurable to decrypt the encrypted broadcast messages.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for: a system for controlling access to broadcast message transmitted over an address and received by several mobile devices.
USE - In personal mobile computing devices for delivering information to, and programming mobile devices.
ADVANTAGE - Provides efficient mechanism by which content messages could be transmitted in a secure fashion
DESCRIPTION OF DRAWING(S) - The drawing shows a flow diagram illustrating programming of a broadcast key into a mobile device.
pp; 98 DwgNo 7/11
Title Terms: ACCESS; BROADCAST; MESSAGE; RECEIVE; NUMBER; MOBILE; DEVICE; CONTROL
Derwent Class: P85; T01; W01; W02; W05
International Patent Class (Main): **H04L-009/00** ; **H04L-009/08** ; **H04L-029/06**
International Patent Class (Additional): G09C-001/00; H04K-001/00; **H04L-012/28** ; H04Q-007/38
File Segment: EPI; EngPI

2/5/29 (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012613347 **Image available**
WPI Acc No: 1999-419451/199935
Related WPI Acc No: 1999-419419; 1999-419431; 1999-419433; 1999-444271; 1999-444272; 2003-361578; 2003-419885
XRPX Acc No: N99-313064

Computer implemented method e.g. for receiving wireless information on portable computer

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: CRONIN D; **KADYK D** ; O'LEARY M J; DEO V; MILLER J M; **TUNIMAN D** ; WECKER D
Number of Countries: 021 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9935778	A2	19990715	WO 99US337	A	19990107	199935	B
EP 1060597	A2	20001220	EP 99901360	A	19990107	200105	
			WO 99US337	A	19990107		
US 6311058	B1	20011030	US 98107666	A	19980630	200172	
JP 2003526226	W	20030902	WO 99US337	A	19990107	200358	

Priority Applications (No Type Date): US 98189591 A 19981110; US 9870720 P 19980107; US 9875123 P 19980213; US 98107666 A 19980630; US 98107724 A 19980630
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9935778	A2	E	85	H04L-000/00	
Designated States (National): CA JP					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 1060597	A2	E		H04L-012/56	Based on patent WO 9935778
Designated States (Regional): DE FR GB					
US 6311058	B1			H04M-003/00	
JP 2003526226	W		89	H04Q-007/38	Based on patent WO 9935778

Abstract (Basic): WO 9935778 A2

NOVELTY - The method involves receiving an information packet comprising a portion having topic information indicative of content in a second portion of the information packet. The first portion of the information packets is compared to content filter data stored on the portable computing device. The second portion of the information packets is forwarded to another component of the portable computing device if the first portion matches any of the content filter data. The information packet is discarded if the first portion does not match any of the content filter data.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for a computer readable medium, a portable computing device, an information packet for transmitting information to a portable computing device, and a computer implemented method for obtaining content filter data on a portable computing device used for processing wireless information.

USE - For receiving wireless information on portable computer.

ADVANTAGE - Efficiently processes information transmitted over wireless channel to mobile device in order to conserve battery resources on computer.

DESCRIPTION OF DRAWING(S) - The figure shows a general structure of a message packet transmitted to the mobile device in accordance with one aspect of the invention.

pp; 85 DwgNo 8/11

Title Terms: COMPUTER; IMPLEMENT; METHOD; RECEIVE; WIRELESS; INFORMATION; PORTABLE; COMPUTER
Derwent Class: W01
International Patent Class (Main): **H04L-000/00** ; **H04L-012/56** ; H04M-003/00; H04Q-007/38
International Patent Class (Additional): **H04L-012/28** ; H04Q-007/14
File Segment: EPI

2/5/30 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012613327 **Image available**
WPI Acc No: 1999-419431/199935
Related WPI Acc No: 1999-419419; 1999-419433; 1999-419451; 1999-444271; 1999-444272; 2003-361578; 2003-419885
XRPX Acc No: N99-313045

Programming interface for transferring information to and from mobile receiver on mobile device e.g. personal digital assistants

Patent Assignee: MICROSOFT CORP (MICT); DEO V (DEOV-I); GOLDSCHMIDT P (GOLD-I); KADYK D (KADY-I); O'LEARY M J (OLEA-I); TUNIMAN D (TUNI-I); O' LEARY M J (LEAR-I)
Inventor: DEO V; **GOLDSCHMIDT P** ; **KADYK D** ; O'LEARY M J; **TUNIMAN D** ; O' LEARY M J
Number of Countries: 021 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week

WO 9935591	A2	1999071[redacted]	WO 99US325	A	19990107	[redacted]9935	B
EP 1053525	A2	20001122	EP 99901356	A	19990107	200061	
			WO 99US325	A	19990107		
US 6282294	B1	20010828	US 9870720	P	19980107	200151	
			US 9874236	P	19980210		
			US 9875123	P	19980213		
			US 98108953	A	19980630		
JP 2002501312	W	20020115	WO 99US325	A	19990107	200207	
			JP 2000527898	A	19990107		
US 20020046343	A1	20020418	US 9870720	P	19980107	200228	
			US 9874236	P	19980210		
			US 9875123	P	19980213		
			US 98108953	A	19980630		
			US 2001764794	A	20010117		
US 20020049905	A1	20020425	US 9870720	P	19980107	200233	
			US 9874236	P	19980210		
			US 9875123	P	19980213		
			US 98108953	A	19980630		
			US 2001761793	A	20010117		
US 20020053025	A1	20020502	US 9870720	P	19980107	200234	
			US 9874236	P	19980210		
			US 9875123	P	19980213		
			US 98108953	A	19980630		
			US 2001764536	A	20010117		

Priority Applications (No Type Date): US 98108953 A 19980630; US 9870720 P 19980107; US 9874236 P 19980210; US 9875123 P 19980213; US 2001764794 A 20010117; US 2001761793 A 20010117; US 2001764536 A 20010117

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9935591	A2	E	88	G06F-017/00	
Designated States (National): CA JP					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 1053525	A2	E		G06F-017/00	Based on patent WO 9935591
Designated States (Regional): DE FR GB					
US 6282294	B1			H04L-009/00	Provisional application US 9870720 Provisional application US 9874236 Provisional application US 9875123
JP 2002501312	W		106	H04L-009/10	Based on patent WO 9935591
US 20020046343	A1			H04L-009/00	Provisional application US 9870720 Provisional application US 9874236 Provisional application US 9875123 Div ex application US 98108953
US 20020049905	A1			H04L-009/00	Provisional application US 9870720 Provisional application US 9874236 Provisional application US 9875123 Div ex application US 98108953 Div ex patent US 6282294
US 20020053025	A1			H04L-009/00	Provisional application US 9870720 Provisional application US 9874236 Provisional application US 9875123 Div ex application US 98108953 Div ex patent US 6282294

Abstract (Basic): WO 9935591 A2

NOVELTY - A device, protocol, network independent mechanism is provided, by which the mobile device (18) can be programmed. Data is encrypted, such that it can be sent in an encrypted and secure fashion from an originator to the mobile device (18).

DETAILED DESCRIPTION - A programming interface enables device/protocol/network independent transmission of messages to, and the programming of, mobile devices (18). Data structures are also maintained on and supported by the mobile device (18). Security is

provided for programming messages and an acknowledgment channel over which the mobile device (18) can acknowledge receipt of, and successful implementation of, a programming message. INDEPENDENT CLAIMS are included for; a computer readable medium comprising a data structure; a transmission system for transmitting information between from an originator to a mobile device; a wireless transmission system for transmitting programming data to a mobile device having a one-way radio receiver.

USE - Broadcasting to, and programming a mobile device in a protocol device e.g. PDAs.

ADVANTAGE - Enables device/protocol/network independent transmission of messages to, and programming of, mobile devices.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of a mobile device in a system according to the invention.

(12) Content provider (10)
Content provider (12)
Wireless carrier (14)
Mobile device (18)
pp; 88 DwgNo 1/12

Title Terms: PROGRAM; INTERFACE; TRANSFER; INFORMATION; MOBILE; RECEIVE; MOBILE; DEVICE; PERSON; DIGITAL; ASSIST

Derwent Class: T01

International Patent Class (Main): G06F-017/00; **H04L-009/00** ; **H04L-009/10**

International Patent Class (Additional): G06F-011/30; G06F-012/14; G06F-013/00; G06F-015/00; G06F-017/60; **H04L-009/32** ; **H04L-013/08** ; **H04L-029/06** ; H04M-001/66

File Segment: EPI

```
Set     Items   Description
S1        807   AU=(TUNIMAN, D? OR TUNIMAN D? OR GOLDSCHMIDT, P? OR GOLDSC-
                HMIDT P? OR O'LEARY, M? OR O'LEARY M? OR KADYK, D? OR KADYK D-
                ?)
S2          4   S1 AND PROTOCOL
S3          0   S1 AND MOBILE()DEVICE?
File   2:INSPEC 1969-2004/Feb W5
         (c) 2004 Institution of Electrical Engineers
File   6:NTIS 1964-2004/Mar W1
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2004/Feb W5
         (c) 2004 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Feb W5
         (c) 2004 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2004/Feb
         (c) 2004 ProQuest Info&Learning
File  65:Inside Conferences 1993-2004/Mar W1
         (c) 2004 BLDSC all rts. reserv.
File  92:IHS Intl.Stds.& Specs. 1999/Nov
         (c) 1999 Information Handling Services
File  94:JICST-EPlus 1985-2004/Feb W5
         (c)2004 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2004/Feb W4
         (c) 2004 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Feb
         (c) 2004 The HW Wilson Co.
File 103:Energy SciTec 1974-2004/Feb B2
         (c) 2004 Contains copyrighted material
File 144:Pascal 1973-2004/Feb W5
         (c) 2004 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2004/Feb 20
         (c) 2004 EBSCO Publishing
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File 239:Mathsci 1940-2004/Apr
         (c) 2004 American Mathematical Society
File 275:Gale Group Computer DB(TM) 1983-2004/Mar 09
         (c) 2004 The Gale Group
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 647:CMP  Computer Fulltext 1988-2004/Feb W5
         (c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Feb W5
         (c) 2004 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2004/Mar 08
         (c) 2004 The Dialog Corp.
```

2/5/1 (Item 1 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci

05791656 Genuine Article#: WX900 Number of References: 20
Title: One course versus two courses of antithymocyte globulin for the treatment of severe aplastic anemia in children
Author(s): Matloub YH (REPRINT) ; Smith C; Bostrom B; Koerper MA; **OLeary M** ; Khuder S; Smithson WA; Nickerson HJ; Silberman T; Hilden J; Moertel CL; Month S; Monteleone P; Ramsay NKC
Corporate Source: MED COLL OHIO,DEPT PEDIAT, DIV PEDIAT HEMATOL ONCOL, 3000 ARLINGTON AVE/TOLEDO//OH/43614 (REPRINT); MED COLL OHIO,DEPT INTERNAL MED/TOLEDO//OH/; CHILDRENS HLTH CARE,/MINNEAPOLIS//MN/; UNIV CALIF SAN FRANCISCO,DIV PEDIAT HEMATOL/SAN FRANCISCO//CA/94143; MAYO CLIN,DIV PEDIAT HEMATOL ONCOL/ROCHESTER//MN/; MARSHFIELD CLIN FDN MED RES & EDUC,/MARSHFIELD//WI/54449; CHILDRENS HLTH CARE,PEDIAT HEMATOL ONCOL/ST PAUL//MN/; OAKLAND KAISER HOSP,/OAKLAND//CA/; BAYSTATE MED CTR,/SPRINGFIELD//MA/; UNIV MINNESOTA,DIV PEDIAT HEMATOL ONCOL/MINNEAPOLIS//MN/55455; UNIV MINNESOTA,DIV PEDIAT BONE MARROW TRANSPLANT/MINNEAPOLIS//MN/55455
Journal: JOURNAL OF PEDIATRIC HEMATOLOGY ONCOLOGY, 1997, V19, N2 (MAR-APR) , P110-114
ISSN: 1077-4114 Publication date: 19970300
Publisher: LIPPINCOTT-RAVEN PUBL, 227 EAST WASHINGTON SQ, PHILADELPHIA, PA 19106
Language: English Document Type: ARTICLE
Geographic Location: USA
Subfile: CC CLIN--Current Contents, Clinical Medicine;
Journal Subject Category: ONCOLOGY; HEMATOLOGY; PEDIATRICS
Abstract: Purpose: The aim of the therapeutic trials was to optimize the treatment of severe aplastic anemia (SAA) and moderate aplastic anemia in children who lack a suitable bone marrow donor, using immunosuppressive therapy in the most effective combination and dose.

Patients and Methods: Two sequential therapeutic trials for the treatment of severe and moderate aplastic anemia in children were conducted by 10 institutions. The treatment protocols included antithymocyte globulin (ATG), prednisone, and cyclosporine A (CSA); patients entered on the first **protocol** , 0190 (ATG x 2), were given two courses of ATG, and those enrolled on the second **protocol** , 0190B (ATG x 1), were given only one course of ATG. Ten patients were evaluable on ATG x 2. All patients had SAA; three had hepatitis-induced severe aplastic anemia (HI-SAA). Twelve patients were evaluable on ATG x 1; all had SAA, one of whom had HI-SAA.

Results: Seven of 10 patients on ATG x 2 responded, and eight of 12 patients treated on ATG x 1 responded.

Conclusion: Treatment with immunosuppressive therapy using ATG, CSA, and prednisone was very well tolerated The response rates in both protocols were similar, and results compare favorably with those of previous therapeutic trials, suggesting that a second course of ATG is not necessary.
Descriptors--Author Keywords: aplastic anemia ; anemia ; aplasia ; antithymocyte globulin ; cyclosporine A
Identifiers--KeyWord Plus(R): BONE-MARROW TRANSPLANTATION; ANDROGENS; THERAPY; ADULTS
Research Fronts: 95-1573 002 (PAROXYSMAL-NOCTURNAL HEMOGLOBINURIA; GLYCOSYLPHOSPHATIDYLINOSITOL MEMBRANE ANCHORS; GPI BIOSYNTHESIS)
Cited References:
ALTER BP, 1978, V7, P431, CLIN HAEMATOL
BACIGALUPO A, 1988, V70, P177, BRIT J HAEMATOL
BAYEVER E, 1984, V105, P920, J PEDIATR
CAMITTA BM, 1974, V43, P473, BLOOD
CAMITTA BM, 1976, V48, P63, BLOOD
CAMITTA BM, 1982, V306, P712, NEW ENGL J MED
CATTRAL MS, 1994, V20, P813, HEPATOLOGY
CHAMPLIN R, 1983, V308, P113, NEW ENGL J MED

DONEY K, 1987, V15, P2[illegible], EXP HEMATOL
FACON T, 1991, V63, P89, ANN HEMATOL
FRICKHOFEN N, P118, APLASTIC ANEMIA CURR
HAGLER L, 1975, V54, P139, MEDICINE
MATLOUB YH, 1994, V16, P104, AM J PEDIAT HEMATOL
MCGLAVE PB, 1987, V70, P1325, BLOOD
NISSEN C, 1992, V83, P319, BRIT J HAEMATOL
PAQUETTE RL, 1995, V85, P283, BLOOD
SANDERS JE, 1994, V16, P43, AM J PEDIAT HEMATOL
SOCIE G, 1993, V329, P1152, NEW ENGL J MED
TICHELLI A, 1988, V69, P413, BRIT J HAEMATOL
WERNER EJ, 1989, V83, P61, PEDIATRICS

2/5/2 (Item 1 from file: 103)

04888168 INIS

Title: Strengthened safeguards: Present and future challenges

Author(s): **Goldschmidt, Pierre** [Department of Safeguards, International Atomic Energy Agency, Vienna (Austria)]
Corporate Source: International Atomic Energy Agency, Vienna (Austria); European Safeguards Research and Development Association, Rome (Italy); Institute of Nuclear Materials Management, Northbrook, IL (United States)

Conference Title: Symposium on international safeguards: Verification and nuclear material security
Conference Location: Austria
Source: Symposium on international safeguards: Verification and nuclear material security, Vienna (Austria), 29 Oct - 2 Nov 2001 ; 1 fig; Data in PDF format; Acrobat Reader for Windows 3.x, 95, 98, NT 3.5.1, NT 4.0, MacIntosh and UNIX (SUN, HP, IRIX (SGI), AIX and Digital UNIX) included; PBD: 2001 ; In: Symposium on international safeguards: Verification and nuclear material security. Proceedings, 1396 pages.
Publication Date: 20010701
Availability Date: 20030120
Report Number(s): IAEA-SM--367/CD; IAEA-SM--367/2/01
OSTI Number(s): DE20282500
Contract Number (Non-DOE): TRN XA0200556045202
Document Type: CONFERENCE
Language: English
Medium/Dimensions: 8 pages
Availability: Available from INIS in electronic form; Also available on 1 CD-ROM from IAEA, Sales and Promotion Unit and on-line at: http://www-pub.iaea.org/MTCD/publications/PDF/SS-2001/Start.pdf. E-mail: sales.publications@iaea.org; Web site: http://www.iaea.org/worldatom/
Country of Publication: Austria

Abstract: The IAEA safeguards system is experiencing what can be seen as a revolution and, in doing so, is confronting a series of challenges. Strengthening measures have meant the availability of more information, increased access to facilities and other locations, and the enhanced use of advanced technology. Implementing these measures has demanded a period of rapid development, which is far from complete. These challenges can be grouped into three areas: drawing and maintaining safeguards conclusions, designing and implementing integrated safeguards, and achieving 'cost neutrality' while maintaining quality and credibility. Implementation of additional protocols represents the most dramatic step the international community has taken over the past decade to strengthen the IAEA safeguards system. However, the full potential of strengthened and integrated safeguards can be realized only when there is universal adherence to the provisions of INFCIRC/540 (Corr.). In 1997, when the Board of Governors approved the Model Additional **Protocol** , there was no shortage of supporting statements by Member States. It is disappointing, therefore, that so many States have been slow in matching their words with deeds. The IAEA safeguards

system is changing and presents many challenges. The Agency is working to meet these challenges and, as experience is gained, the planning and implementation measures are being further developed. At the same time, safeguards activities continue to be conducted, covering the 352 facilities with one significant quantity or more of nuclear material. The fact that the Agency is managing to conduct these activities with historically high levels of success while facing all the challenges that have been outlined is an achievement in which the Agency can take pride.
Descriptors: ARMS CONTROL; IAEA AGREEMENTS; IAEA SAFEGUARDS; IMPLEMENTATION ; INSPECTION; NUCLEAR WEAPONS; PHYSICAL PROTECTION; RECOMMENDATIONS; SABOTAGE; SECURITY
Subject Categories: 98 -- NUCLEAR DISARMAMENT, SAFEGUARDS, & PHYSICAL PROTECTION

2/5/3 **(Item 2 from file: 103)**
DIALOG(R)File 103:Energy SciTec

04777925 RN02011970; TVI 3307; TRN XA0200006006892; INIS
Title: Strengthened safeguards: Present and future challenges
Author(s): **Goldschmidt, Pierre** [International Atomic Energy Agency, Vienna (Austria)]
Corporate Source: International Atomic Energy Agency, Vienna (Austria); European Safeguards Research and Development Association, Rome (Italy); Institute of Nuclear Materials Management, Northbrook, IL (United States)
Conference Title: Symposium on international safeguards: Verification and nuclear material security
Conference Location: Austria
Source: Symposium on international safeguards: Verification and nuclear material security, Vienna (Austria), 29 Oct - 2 Nov 2001 ; PBD: 2001 ; In: Symposium on international safeguards: Verification and nuclear material security. Book of extended synopses, 377 pages.
Publication Date: 20010701
Availability Date: 20020304
Report Number(s): IAEA-SM--367; IAEA-SM--367/2/01
OSTI Number(s): DE20229274
Contract Number (Non-DOE): TRN XA0200006006892
Document Type: CONFERENCE
Language: English
Medium/Dimensions: page(s) 11
Availability: Available from INIS in electronic form
Country of Publication: Austria
Abstract: Full text: The safeguards system is experiencing what has been seen as a revolution and, in doing so, it is confronting a series of challenges. These can be grouped into three areas. Drawing and maintaining safeguards conclusions - The process by which the safeguards conclusions are derived is based upon the analysis, evaluation and review of all the information available to the Agency. This process is on- going, but the State Evaluation Reports are compiled and reviewed periodically. For States with an additional **protocol** in force, the absence of indicators of the presence of undeclared nuclear material or activities provides the basis for the safeguards conclusion. Future challenges center on States' expectations of, and reactions to, the results of the evaluation and review process. Designing and implementing integrated safeguards - The conceptual framework of integrated safeguards is being actively pursued. Basic principles have been defined and integrated safeguards approaches have been developed for various types of facilities. Work is also progressing on the design of integrated safeguards approaches for specific States. Complementary access is being successfully implemented, and procedures for the use of unannounced inspections are being developed with the prospect of cost- effectiveness gains. Costs neutrality vs. quality and credibility - The Department faces serious staff and financial challenges. It has succeeded so far in 'doing more'

and 'doing better' with a zero-real growth budget, but the scope for further significant efficiency gains is exhausted. There is no capacity to absorb new or unexpected tasks. Difficulties in recruiting and retaining qualified and experienced staff exacerbate the problems and add to costs. The Director General of the IAEA has referred to the need for new initiatives to bridge the budgetary gap; a possible measure is proposed. The tasks of meeting the challenges and demands of strengthened safeguards have been added to the tasks of implementing traditional safeguards. New tasks are appearing; a significant recent example is the consequence, for the Department's Security of Material Programme, of the September terrorist attacks in the United States. The gap between what is required and the available resources cannot continue to increase indefinitely. (author)
Descriptors: BUDGETS; EFFICIENCY; EVALUATION; IAEA SAFEGUARDS; INFORMATION NEEDS; SECURITY
Subject Categories: 98 -- NUCLEAR DISARMAMENT, SAFEGUARDS, & PHYSICAL PROTECTION

2/5/4 (Item 3 from file: 103)
DIALOG(R)File 103:Energy SciTec

04631045 EDB-00-101451
Title: The basis for the strengthening of safeguards
Author(s): **Goldschmidt, P.** (International Atomic Energy Agency, Department of Safeguards, Vienna (Austria))
Title: IAEA safeguards for the 21st century
Corporate Source: International Atomic Energy Agency, Vienna (Austria) Ministry of Science and Technology (MOST), Taejon (Korea, Republic of)
Conference Title: Seminar on IAEA safeguards for the 21st century
Conference Location: Taejon (Korea, Republic of) Conference Date: 18 - 20 Oct 1999
Publication Date: 1999
p [22] ([271] p)
Report Number(s): INIS-XA-219 M2.49-ROK/SSAC--99
Document Type: Analytic of a Report; Conference Literature; Special Availability
Language: English
Journal Announcement: EDB0022
Availability: Available from INIS in electronic form
Subfile: ETD (Energy Technology Data Exchange). INIS (non-US Atomindex input AIX)
Country of Origin: International Atomic Energy Agency (IAEA)
Country of Publication: International Atomic Energy Agency (IAEA)
Abstract: For the past 30 years, the International Atomic Energy Agency's safeguards system has contributed to the international non-proliferation regime, by providing, inter alia, assurances regarding the peaceful uses of declared nuclear material. However, the discovery of a clandestine nuclear weapons programme in Iraq in 1991 drew world-wide attention to the need to strengthen the system to address the absence of undeclared nuclear material and activities. Efforts to strengthen the IAEA's safeguards system began in 1991 and culminated in 1997 when the IAEA's Board of Governors approved a Model **Protocol** Additional to IAEA Safeguards Agreements which greatly expands the legal basis and scope of IAEA safeguards. Within this strengthened system it is expected that the IAEA be able to provide assurance not only of the absence of diversion of declared nuclear material but also on the absence of undeclared nuclear material and activities. This is to be done within a safeguards system that uses an optimal combination of all safeguards measures available, thereby achieving maximum effectiveness and efficiency within the available resources. This paper will summarize the evolution of the safeguards system, describe strengthened safeguards, report on the status of implementing the strengthening measures, and outline plans for integrating all available safeguards measures. (author)
Descriptors: AGREEMENTS; ARMS CONTROL; IAEA AGREEMENTS; IAEA SAFEGUARDS;

IMPLEMENTATION; INSPECTION; NON-PROLIFERATION POLICY; NUCLEAR MATERIALS DIVERSION
Broader Terms: INTERNATIONAL AGREEMENTS; SAFEGUARDS; AGREEMENTS
Subject Categories: 056000* -- Nuclear Fuels -- Legislation & Regulations -- (1987-)

```
Set     Items   Description
S1       6751   (ENCRYPT? OR ENCODE? OR CIPHER OR CIPHERS OR SECURITY)(2N)-
            (KEY OR KEYS)
S2    3587639   FIRST OR 1ST OR PRIME OR PRIMARY OR INITIAL OR MAIN OR ORI-
            GINAL
S3    2574799   SECOND OR 2ND OR ANOTHER OR ADDITIONAL
S4       5888   (BASE OR SHARED OR PRIVATE OR LOCAL OR MASTER OR PUBLIC)(2-
            N)(KEY OR KEYS) OR PKI
S5      32127   (DATA OR INFORMATION)()(STREAM? OR STRING? OR SEGMENT? OR -
            PIECE? OR PART? OR CHUNK? OR BLOCK?)
S6      16956   (DATA OR INFORMATION)()(PART? OR SEGMENT? OR PORTION? OR P-
            IECE? OR MESSAGE()SPECIFIC OR SIGNATURE OR IDENTIF? OR ID)
S7       2269   (HASH? OR KEY()SPLITTING OR CHECKSUM OR ONE()WAY()FUNCTION
            OR ALGORITHM?)(2N)(DATA OR INFORMATION OR DIGEST? OR FINGERPR-
            INT? OR FINGER()PRINT?)
S8        220   S2 (2W)S1
S9         37   S8 AND S4
S10      2006   S2 (3N) S5
S11         0   S9 AND S10 AND S6
S12         1   S9 AND S6
S13         0   S9 AND S10
S14         3   S8 AND S10
S15         3   S8 AND S6
S16         7   S8 AND S7
S17   6451929   DERIVE? OR OBTAIN? OR RECEIVE? OR DERIVE? OR DRAW? OR GET -
            OR TAKE?
S18       207   S3 (2W) S1
S19       161   S18 AND S17
S20       161   S19 AND S1
S21        36   S20 AND S4
S22      1090   S3 (2N) S5
S23       236   S22 AND S6
S24         1   S23 AND S7
S25        50   S12 OR S14 OR S15 OR S16 OR S21 OR S24
S26        49   S25 AND IC=(G06F? OR H04L? OR H04M?)
S27         0   S25 AND MC=T01-J
S28    478563   (MOBILE OR PORTABLE OR CELLULAR OR CELL OR WIRELESS)(2W)(D-
            EVICE? OR CLIENT? OR NODE? OR TELECOMMUNICATION? OR COMPUTER?
            OR PHONE? OR TELEPHONE? OR TERMINAL) OR CELLPHONE? OR CELL()P-
            HONE? OR WIRELESS OR WIRE()LESS OR RADIO?
S29         3   S26 AND S28
S30        49   S26 OR S29
File 347:JAPIO Nov 1976-2003/Nov(Updated 040308)
        (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200416
        (c) 2004  THOMSON DERWENT
```

The subscriber office decodes the **received** authentication request using the first **encryption key**, recognizes it as the authentication request, and transmits an authentication response encrypted using the first **encryption key** to the **base** station. The base station decodes the **received** authentication response using the **second encryption key** to recognize the validity of the authentication response.

30/5/3 (Item 3 from file: 347)
DIALOG(R)File 347:JAPIO

07047152 **Image available**
CONTENTS INFORMATION TRANSMISSION METHOD, CONTENTS INFORMATION RECORDING METHOD, CONTENTS INFORMATION TRANSMITTER, CONTENTS INFORMATION RECORDER, TRANSMISSION MEDIUM AND RECORDING MEDIUM

PUB. NO.: 2001-274786 [JP 2001274786 A]
PUBLISHED: October 05, 2001 (20011005)
INVENTOR(s): KUROIWA TOSHIO
SUGAWARA TAKAYUKI
IBA WATARU
UEDA KENJIRO
HIGURE SEIJI
APPLICANT(s): VICTOR CO OF JAPAN LTD
APPL. NO.: 2000-051204 [JP 200051204]
FILED: February 28, 2000 (20000228)
PRIORITY: 2000-012733 [JP 200012733], JP (Japan), January 21, 2000 (20000121)
INTL CLASS: **H04L-009/08** ; **G06F-015/00** ; G09C-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To provide a contents information transmission method, the recording method, transmitter, recorder, transmission medium and recording medium thereof, by which a decoder side cannot respectively identify key generating algorithms used for encryption according to each designated algorithm number only with the intelligence given to an encryption side, so as to more vigorously prevent unauthorized reproduction and copy of contents information, thereby enhancing copyright protection.

SOLUTION: The method adopts transmission or recording of encrypted contents information resulting from encrypting contents information, by using a 1st key generated from source information of the 1st key, source information of an **encrypted 1st key** resulting from **encrypting** source information of the 1st key, using a 2nd key generated by a prescribed key generating algorithm on the basis of a given initial value, **algorithm** identification **information** for identifying the prescribed by generating algorithm and initial value information denoting the initial value.

30/5/4 (Item 4 from file: 347)
DIALOG(R)File 347:JAPIO

06962153 **Image available**
METHOD AND DEVICE FOR GENERATING DISTRIBUTED CRYPTOGRAPHIC KEY, AND RECORDING MEDIUM RECORDED WITH DISTRIBUTED CRYPTOGRAPHIC KEY GENERATION PROGRAM

PUB. NO.: 2001-189719 [JP 2001189719 A]
PUBLISHED: July 10, 2001 (20010710)
INVENTOR(s): TAKAGI TAKESHI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP (NTT)

APPL. NO.: 11-375847 [JP 99375847]
FILED: December 28, 1999 (19991228)
INTL CLASS: **H04L-009/08** ; G09C-001/00; **H04L-009/30**

ABSTRACT

PROBLEM TO BE SOLVED: To provide a method and a device capable of generating a distributed cryptographic key at a higher speed as compared with the conventional distributed key generating method, and to provide a recording medium in which the program therefor is recorded.

SOLUTION: This distributed cryptographic key generating device in an enciphering device has i-pieces (i=1, 2,..., k) of cryptographic key generating means (i) for generating the cryptographic keys by setting p2q as a 1st **public key** (n) with pi and qi (where p=Σ pi and q=Σ qi) **obtained** by distributing two prime numbers (p) and (q) to a server (i) as a 1st distributed secret key, setting (e) satisfying ed = 1 mod L (where L=p(p-1)(q-1) as a 2nd **public key** and setting di (where d=Σ di) **obtained** by distributing (d) to the server (i) as a **2nd** distributed secret **key** , and **obtains cipher** text C based on C=Me (mod n) from plaintext M by using the 1st and 2nd **public keys** (n) and (e) generated by the means (i). Each of cryptographic key generating means (i) is provided with a random number generating means for respectively generating two random numbers pi and qi and a **public key** candidate generating means for generating candidates N=(Σi1, 2,..., kpi)2 (Σi1, 2,..., kqi) for the 1st **public key** (n) by using a BGW protocol.

30/5/5 (Item 5 from file: 347)
DIALOG(R)File 347:JAPIO

06222288 **Image available**
GENERATING SYSTEM FOR ENCRYPTION KEY, ITS GENERATOR AND ENCRYPTION KEY GENERATING RECORDING MEDIUM

PUB. NO.: 11-163850 [JP 11163850 A]
PUBLISHED: June 18, 1999 (19990618)
INVENTOR(s): TANAKA HATSUICHI
INOUE TORU
APPLICANT(s): KODO IDO TSUSHIN SECURITY GIJUTSU KENKYUSHO KK
APPL. NO.: 09-343604 [JP 97343604]
FILED: December 01, 1997 (19971201)
INTL CLASS: **H04L-009/08** ; G09C-001/00; **H04L-009/10**

ABSTRACT

PROBLEM TO BE SOLVED: To provide a generating system for an encryption key where a common encryption key is easily generated and the secrecy is easily managed.

SOLUTION: A **1st encryption key** generating section 1 receives 1st data and ID information IDB of a user B, generates an encryption key KAB(A) of a user A by a 2nd algorithm, and a 2nd encryption key generating section 2 receives 2nd data and ID information IDA of a user A, generates an encryption key KABB of a user B by the 2nd **algorithm** . The 1st **data** are generated by a 1st algorithm 3 based on the ID information IDA of the user A and a random number. The 2nd data are generated by the 1st algorithm 3 based on the ID information IDB of the user B and the random number. The encryption key KAB(A) of the user A and the encryption key KAB(B) of the user B are identical to each other.

30/5/6 (Item 6 from file: 347)

DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

02852036 **Image available**
PRIVACY TELEPHONE SYSTEM

PUB. NO.: 01-149636 [JP 1149636 A]
PUBLISHED: June 12, 1989 (19890612)
INVENTOR(s): NAKAJIMA SHIGEO
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 62-307646 [JP 87307646]
FILED: December 07, 1987 (19871207)
INTL CLASS: [4] **H04L-009/02**
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 34.4 (SPACE DEVELOPMENT -- Communication)
JOURNAL: Section: E, Section No. 819, Vol. 13, No. 410, Pg. 77, September 11, 1989 (19890911)

ABSTRACT

PURPOSE: To safely transmit a **cipher key** and at the same time, to easily encode and decode information data by protecting the information data themselves with the 1st **cipher key** and transmission of the 1st **cipher key** itself by means of **another cipher key** .

CONSTITUTION: Assuming that earth stations A and B respectively have 1st **cipher keys** MA and MB for making information signals **private** , transmission **keys** KAR and KBT for making the 1st **cipher keys private** , and reception **keys** KAR and KBR, the station B produces a call signal to the station A and simultaneously transmits the KBT when the station B makes an originating call. At the station A, upon receiving the KBT, one is selected out of plural MAs and the selected MA is made private by using the KBT. Then the private MA is transmitted to the station B together with the KAT. At the station B, the **received** signals are decoded by using the reception key KBR and the MA is **obtained** . Moreover, one is selected out of plural MBs and the selected MB is made private by using the **received** KAR. The private MB is transmitted to the station A. At the station A, the **received** signal is decoded by using the reception key KAR and the MB is **obtained** . At both stations A and B, the initial data of the scramble of transmitting information data for the stations B and A are set by using the **received** MB and MA, respectively.

30/5/7 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 THOMSON DERWENT. All rts. reserv.

015904779 **Image available**
WPI Acc No: 2004-062619/200406
XRPX Acc No: N04-050597
Method of secure data exchange between two devices, used in pay-per-view television systems, has security module generating encrypted random number, which is decrypted by receiver **, and vice versa**
Patent Assignee: NAGRACARD SA (NAGR-N)
Inventor: BRIQUE O; NICOLAS C; SASSELLI M
Number of Countries: 103 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 2003107585	A1	20031224	WO 2003IB2425	A	20030610	200406	B

Priority Applications (No Type Date): CH 20021002 A 20020612
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 2003107585	A1	F	27	H04L-009/08	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO

NZ OM PH PL PT RO RU SC[redacted]D SE SG SK SL TJ TM TN TR TT TZ[redacted]A UG US UZ VC VN YU ZA ZM ZW
Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW

Abstract (Basic): WO 2003107585 A1

NOVELTY - The first device (10) is a security module containing a first **encryption key**, called **private key** (PAKV) of a pair of asymmetric **encryption keys**. The second device is a **receiver** (11) comprising at least a **second encryption key**, called **public key** (PAKB) of the pair of asymmetric **encryption keys**. Each of the devices further comprises a symmetric key (13). The first device (10) generates a first random number (A), which is encrypted by the **private key** (PAKV), then transmitted to the second device (11), wherein it is decrypted by means of the **public key** (PAKB).

DETAILED DESCRIPTION - The second device (11) generates a second random number (B), which is encrypted by the **public key** (PAKB), then transmitted to the first device (10), where it is decrypted by the **private key** (PAKV). A session key (SK), used for secure data exchanges, is generated by a combination of the symmetric key and the random numbers (A, B) generated and **received** by each of the devices.

USE - For secure data exchange between two locally interconnected devices, e.g. a **receiver** and a security module, used especially in the field of pay-per-view television services.

ADVANTAGE - The unauthorised decoding of such services is particularly complex as to be virtually impossible.

DESCRIPTION OF **DRAWING** (S) - The **drawing** is a schematic layout of the data exchange system.

first device (10)
second device (**receiver**) (11)
symmetric key (13)
private key (PAKV)
public key (PAKB)
session key (SK)
random numbers (A,B)
pp; 27 DwgNo 4/4

Title Terms: METHOD; SECURE; DATA; EXCHANGE; TWO; DEVICE; PAY; PER; VIEW; TELEVISION; SYSTEM; SECURE; MODULE; GENERATE; ENCRYPTION; RANDOM; NUMBER; **RECEIVE** ; VICE
Derwent Class: W01; W02
International Patent Class (Main): **H04L-009/08**
International Patent Class (Additional): H04N-007/16
File Segment: EPI

30/5/8 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015463442 **Image available**
WPI Acc No: 2003-525584/200350
Related WPI Acc No: 2003-515586; 2003-525583; 2003-543781; 2003-543782; 2003-543783; 2003-543784; 2003-543785; 2003-543786; 2003-560680; 2003-597683
XRPX Acc No: N03-417066

Secured file format for electronic digital data in enterprise computer system encrypts data using integration of header, containing first **and second** encrypted security keys **, and file data encrypted by** first security key

Patent Assignee: PERVASIVE SECURITY SYSTEMS INC (PERV-N)
Inventor: GARCIA D J P
Number of Countries: 031 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1326157	A2	20030709	EP 2002258536	A	20021211	200350	B
JP 2003218851	A	20030731	JP 2002359963	A	20021211	200351	

Priority Applications (No Type Date): US 2002159537 A 20020531; US 2001339634 P 20011212; US 200274804 A 20020212
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
EP 1326157 A2 E 23 G06F-001/00
Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR
JP 2003218851 A 21 H04L-009/08

Abstract (Basic): EP 1326157 A2
NOVELTY - File data is stored in a format which integrates an encrypted header (110) and an encrypted **data portion** (112) to generate a secured file (108). The header includes two security keys with the **first key encrypted** by the second key and the second key encrypted and guarded by encrypted access rules (104).
DETAILED DESCRIPTION - The encrypted **data portion** is generated by encrypting the created document data (100) with the **first security key** according to a pre-determined cipher scheme.
INDEPENDENT CLAIMS are also include for ;
(1) A method for securing electronic data in a format.
(2) Stored software.
USE - For protecting and securing digital electronic data in an enterprise environment.
ADVANTAGE - The digital electronic data is stored in a secure format accessible only by users having the appropriate granted access rights and security keys.
DESCRIPTION OF DRAWING(S) - The drawing shows a flow diagram for securing a created document according to a secured file form.
Created document data (100)
Encrypted access rules (104)
Secured file (108)
Encrypted header (110)
Encrypted **data portion** (112)
pp; 23 DwgNo 1/6
Title Terms: SECURE; FILE; FORMAT; ELECTRONIC; DIGITAL; DATA; COMPUTER; SYSTEM; DATA; INTEGRATE; HEADER; CONTAIN; FIRST; SECOND; ENCRYPTION; SECURE; KEY; FILE; DATA; ENCRYPTION; FIRST; SECURE; KEY
Derwent Class: P85; T01
International Patent Class (Main): **G06F-001/00 ; H04L-009/08**
International Patent Class (Additional): **G06F-012/00 ; G06F-012/14 ;** G09C-001/00
File Segment: EPI; EngPI

30/5/9 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015271275 **Image available**
WPI Acc No: 2003-332204/200331
XRPX Acc No: N03-266251
Conducting method for private secure electronic commerce, involves adjusting value parameter in response to provision of encrypted data communications to user
Patent Assignee: ALLDREDGE R L (ALLD-I)
Inventor: ALLDREDGE R L
Number of Countries: 001 Number of Patents: 001
Patent Family:
Patent No Kind Date Applicat No Kind Date Week
US 20030046534 A1 20030306 US 2001944761 A 20010831 200331 B

Priority Applications (No Type Date): US 2001944761 A 20010831
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
US 20030046534 A1 17 G06F-017/60

Abstract (Basic): US 200[redacted]6534 A1

NOVELTY - The method involves adjusting the value parameter in response to the provision of encrypted data communications to a user. The encrypted data communications are provided to the user until the value parameter is exhausted. The value parameter is associated with a sequence of **encryption key** provided to an anonymous user in exchange for a payment.

DETAILED DESCRIPTION - The sequence of **encryption key** is used for decrypting a message that has been encrypted using **another** sequence of **encryption key** . The other sequence of **encryption key** is used for decrypting the message that has been encrypted using the sequence of **encryption key** . INDEPENDENT CLAIMS are also included for the following:

(a) an apparatus for conducting secured electronic commerce; and

(b) a **portable** storage **device** .

USE - Used for conducting private secure electronic commerce over the Internet.

ADVANTAGE - Assures that a user remains anonymous to the encryption server as well as any party that might intercept the encrypted data. Provides a reliable and secure way of serving users and service providers throughout the world. Eases access to the seller's **public key** since the sellers have the option to use a single **public private key** pair on a permanent basis. Enables a vendor to reliably **receive** payment for sold product. Eliminates the ability of hackers to know the content of a transaction. Protects the user and the content's of the user transaction from unauthorized disclosure.

DESCRIPTION OF **DRAWING** (S) - The figure shows the schematic block diagram of the method for conducting private secure electronic commerce.

pp; 17 DwgNo 1/2

Title Terms: CONDUCTING; METHOD; PRIVATE; SECURE; ELECTRONIC; ADJUST; VALUE ; PARAMETER; RESPOND; PROVISION; ENCRYPTION; DATA; COMMUNICATE; USER

Derwent Class: T01; T05; W01

International Patent Class (Main): **G06F-017/60**

File Segment: EPI

30/5/10 (Item 4 from file: 350)

DIALOG(R)File 350:Derwent WPIX

015252592 **Image available**

WPI Acc No: 2003-313518/200330

XRPX Acc No: N03-249582

Secrete communication method e.g. for providing confidentiality of message which are sent via communication lines, involves secret communication between transmitting unit and receiving unit

Patent Assignee: GRAVITON HB (GRAV-N)

Inventor: KUTCHEROV V; POTAPKIN A

Number of Countries: 100 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200326199	A1	20030327	WO 2002SE1623	A	20020909	200330	B

Priority Applications (No Type Date): US 2001323640 P 20010920

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200326199	A1	E	21	H04L-009/30	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW

Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SK SL SZ TR TZ UG ZM ZW

Abstract (Basic): WO 200326199 A1

NOVELTY - The method involves a secret communication between a transmitting unit and a receiving unit. The first time any message is sent from the transmitting unit to the receiving unit, the units are synchronized. The transmitting unit generates a **public key** (16) and a **security key** (17a). A message (15) is encrypted using the **public key** and the first **security key** . The **encrypted** message (18) and the **public key** are sent via a transmitting medium. The first **security key** is not sent to the receiving unit. Upon receipt, the receiving unit generates a **second security key** that is identical to the first **security key** . The receiving unit decrypts the message to the readable message using the **public key** and the **second security key** .

USE - For providing confidentiality of message which are sent via communication lines

ADVANTAGE - Provides increased encrypting durability of communication and excludes possibility of unauthorized access to transmitted information. Simple and reliable

DESCRIPTION OF **DRAWING** (S) - The figure shows a flow chart of an implementation system of the invention.

Message (15)

Public key (16)

Security key (17a)

Encrypted message (18)

pp; 21 DwgNo 1/2

Title Terms: SECRETION; COMMUNICATE; METHOD; CONFIDE; MESSAGE; SEND; COMMUNICATE; LINE; SECRET; COMMUNICATE; TRANSMIT; UNIT; **RECEIVE** ; UNIT

Derwent Class: W01

International Patent Class (Main): **H04L-009/30**

File Segment: EPI

30/5/11 (Item 5 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014930278 **Image available**

WPI Acc No: 2002-750987/200281

XRPX Acc No: N02-591452

Encryption system has step where If stored, the first encryption **session** key **is decrypted by an inherent key corresponding to the creator ID in the management database**

Patent Assignee: PUMPKIN HOUSE INC (PUMP-N)

Inventor: SASAKI M

Number of Countries: 025 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200287146	A1	20021031	WO 2002JP1996	A	20020305	200281	B

Priority Applications (No Type Date): JP 2001120327 A 20010418

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200287146	A1	J	195	H04L-009/08	

Designated States (National): AU CA CN JP KR US

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

Abstract (Basic): WO 200287146 A1

NOVELTY - An encryption system can flexibly modify a decoding authority and prevent unauthorized use by a third person. When an encryption file is accepted by a client, a decryption executer ID, a creator ID, and a first **encryption** session **key** are transmitted to a key management server (10) (step 141). Check is made whether the creator ID is stored as a decryption object ID in a management database corresponding to the decryption executer ID (step 147).

DETAILED DESCRIPTION - If stored, the first **encryption** session **key** is decrypted by an inherent key corresponding to the creator ID in the management database (step 148). The session **key obtained** is **encrypted** by a **public key** corresponding to the decryption executer

ID (step 149). At the client who has **received** this **second encryption** session **key** , decryption is performed by using a secret key so as to **obtain** the session **key** . **Encrypted** data is decrypted by using the session key.

DESCRIPTION OF **DRAWING** (S) - first **encryption** session **key** are transmitted to a key management server (10) (step 141)

Check is made whether the creator ID is stored as a decryption object ID in a management database corresponding to the decryption executer ID (step 147)

If stored, the first **encryption** session **key** is decrypted by an inherent key corresponding to the creator ID in the management database (step 148)

Session **key** **obtained** is **encrypted** by a **public** **key** corresponding to the decryption executer ID (step 149)

pp; 195 DwgNo 9/51

Title Terms: ENCRYPTION; SYSTEM; STEP; STORAGE; FIRST; ENCRYPTION; SESSION; KEY; INHERENT; KEY; CORRESPOND; CREATION; ID; MANAGEMENT; DATABASE

Derwent Class: T01; W01

International Patent Class (Main): **H04L-009/08**

File Segment: EPI

30/5/12 (Item 6 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014900452 **Image available**

WPI Acc No: 2002-721158/200278

Double encoding and transmitting/receiving method for private **key** **movement and roaming service in** public **key** **based configuration**

Patent Assignee: SECUI.COM CORP (SECU-N)

Inventor: HUH W G

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
KR 2002042083	A	20020605	KR 200071821	A	20001130	200278 B

Priority Applications (No Type Date): KR 200071821 A 20001130

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2002042083	A		1	H04L-009/32	

Abstract (Basic): KR 2002042083 A

NOVELTY - A double encoding and transmitting/receiving method for a **private** **key** movement and roaming service in a **public** **key** based configuration is provided to **draw** out a **private** **key** through a stable communication channel by doubly encoding and entrusting a user's **private** **key** to a roaming service center.

DETAILED DESCRIPTION - A user firstly encodes one's **private** **key** as a password using a personal computer(S101). The user requests a roaming service center to authenticate a **public** **key** (S102). A roaming service center authenticates the user and issues a note of authentication(S103). The user secondly **encodes** a **public** **key** of the roaming service center(S104). The user transmits an identification authenticated by the roaming service center to a server of the roaming service center(S105). The server of the roaming service center stores an N value, a **second** **encoded** **private** **key** , and identification(S106). When the user requests the roaming service center to **draw** out a **private** **key** , the server of the roaming service center forms a stable communication channel, and requests the user to input the identification and a password. The user inputs and transmits the identification and the password to the roaming service center. The server of the roaming service center detects the identification which the user inputs and detects the **second** **encoded** **private** **key** from a double **encoded** **private** **key** .

pp; 1 DwgNo 1/10

Title Terms: DOUBLE; ENCODE; TRANSMIT; **RECEIVE** ; METHOD; PRIVATE; KEY;

MOVEMENT; SERVICE; PUBLIC; KEY; BASED; CONFIGURATION
Derwent Class: W01
International Patent Class (Main): **H04L-009/32**
File Segment: EPI

30/5/13 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014900285 **Image available**
WPI Acc No: 2002-720991/200278
Double encoding and transmitting/receiving method for private key **movement and roaming service in** public key **based configuration**
Patent Assignee: SECUI.COM CORP (SECU-N)
Inventor: HUH W G
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2002041857	A	20020605	KR 200071471	A	20001129	200278	B

Priority Applications (No Type Date): KR 200071471 A 20001129
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2002041857	A		1	H04L-009/32	

Abstract (Basic): KR 2002041857 A
NOVELTY - A double encoding and transmitting/receiving method for a **private key** movement and roaming service in a **public key** based configuration is provided to **draw** out a **private key** through a stable communication channel by doubly encoding and entrusting a user's **private key** to a roaming service center.
DETAILED DESCRIPTION - A user firstly encodes one's **private key** as a password using a personal computer(S101). The user requests a roaming service center to authenticate a **public key** (S102). A roaming service center authenticates the user and issues a note of authentication(S103). The user secondly **encodes** a **public key** of the roaming service center(S104). The user transmits an identification authenticated by the roaming service center to a server of the roaming service center(S105). The server stores the **second encoded private key** and identification in a double encoding **private key** database and an identification database, respectively(S106). When the user requests the roaming service center to **draw** out a **private key** (S107), the server forms a stable communication channel(S108), and requests the user to input the identification and a password(S109). The user inputs and transmits the identification and the password to the roaming service center(S110). The server detects the identification which the user inputs(S111) and decodes the **second encoded private key** to a **private key** of the roaming service center(S112). The roaming service center judges whether the decoded identification is identical with the identification which the user has inputted(S113).
pp; 1 DwgNo 1/10
Title Terms: DOUBLE; ENCODE; TRANSMIT; **RECEIVE** ; METHOD; PRIVATE; KEY; MOVEMENT; SERVICE; PUBLIC; KEY; BASED; CONFIGURATION
Derwent Class: W01
International Patent Class (Main): **H04L-009/32**
File Segment: EPI

30/5/14 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014862897 **Image available**
WPI Acc No: 2002-683603/200274
XRPX Acc No: N02-539641
Computer-aided encryption key **generation method provides** public

encryption key with common first part and second part specific to each receiver

Patent Assignee: DEUT TELEKOM AG (DEBP)
Inventor: MERZENICH K
Number of Countries: 022 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 10114157	A1	20020926	DE 1014157	A	20010322	200274	B
WO 200278246	A2	20021003	WO 2002DE877	A	20020312	200275	
EP 1374479	A2	20040102	EP 2002729776	A	20020312	200409	
			WO 2002DE877	A	20020312		

Priority Applications (No Type Date): DE 1014157 A 20010322
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 10114157	A1		6	H04L-009/30	
WO 200278246	A2	G		H04L-009/00	
Designated States (National): CA US					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR					
EP 1374479	A2	G		H04L-009/30	Based on patent WO 200278246
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR					

Abstract (Basic): DE 10114157 A1

NOVELTY - The **encryption key** generation method provides a **public encryption key** (14) which has a first part (18) which is common to all **receivers** (12,12',12'') for the encrypted information and a second part (20) calculated via data specific to each **receiver**, with a **private key** (16,16',16'') for deciphering of the information transmitted to each **receiver** by a key distribution center (22).

USE - The method is used for computer-aided generation of a **public encryption key** for transmission of sensitive information.

ADVANTAGE - The method allows a separate **encryption key** to be provided for each **receiver** with minimum memory requirement.

DESCRIPTION OF **DRAWING** (S) - The figure shows a schematic representation of a computer-aided **encryption key** generation method.

Receivers (12,12',12'')
Public encryption key (14)
Private keys (16,16',16'')
First part of **encryption key** (18)
Second part of **encryption key** (20)
Key distribution center (22)
pp; 6 DwgNo 1/1

Title Terms: COMPUTER; AID; ENCRYPTION; KEY; GENERATE; METHOD; PUBLIC; ENCRYPTION; KEY; COMMON; FIRST; PART; SECOND; PART; SPECIFIC; **RECEIVE**
Derwent Class: W01
International Patent Class (Main): **H04L-009/00** ; **H04L-009/30**
File Segment: EPI

30/5/15 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014593733 **Image available**
WPI Acc No: 2002-414437/200244
XRPX Acc No: N02-325861

Service issue method for shops and entrance gate, involves providing service to user by encrypting user identification information

Patent Assignee: HITACHI LTD (HITA); HIRANO M (HIRA-I); IWAMURA M (IWAM-I); MATSUKI T (MATS-I); NOYAMA H (NOYA-I); TERADA S (TERA-I)
Inventor: HIRANO M; IWAMURA M; MATSUKI T; NOYAMA H; TERADA S
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week

US 20020034305 A1 20020321 US 2001908719 A 20010720 200244 B
JP 2002117350 A 20020419 JP 2001217507 A 20010718 200244

Priority Applications (No Type Date): JP 2000226185 A 20000721
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
US 20020034305 A1 21 H04L-009/00
JP 2002117350 A 14 G06F-017/60

Abstract (Basic): US 20020034305 A1
NOVELTY - An identification information (ID) (1130) is generated in response to a service application filed by an user to a service issue system (1110). The generated information is encrypted using a **private key** (1140) of the service issue system. The encrypted data (1160) is again encrypted by **another encryption key** of the user, and is output to the user.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(a) Service issue system;
(b) Ticket issue method;
(c) Ticket issue system;
(d) Service providing method;
(e) Service providing system;
(f) User application receiving method;
(g) User application receiving system
USE - For issuing services after user's authentication, in shops and entrance gates.
ADVANTAGE - Enables to determine user identity or the user's rights are legitimate or not even in a place of use, where the database of the user or a sufficient network cannot be installed, hence even a shop of low reliability can be used as a place where transactions are positively substantiated by suppressing illegal act.
DESCRIPTION OF **DRAWING** (S) - The figure shows the flowchart of the service issuing method.
Service issue system (1110)
Identification information (1130)
Private key (1140)
Encrypted data (1160)
pp; 21 DwgNo 1/12
Title Terms: SERVICE; ISSUE; METHOD; SHOP; ENTER; GATE; SERVICE; USER; USER ; IDENTIFY; INFORMATION
Derwent Class: P85; T01; T05; W01
International Patent Class (Main): **G06F-017/60** ; **H04L-009/00**
International Patent Class (Additional): G09C-001/00; **H04L-009/14** ; **H04L-009/32**
File Segment: EPI; EngPI

30/5/16 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014261065 **Image available**
WPI Acc No: 2002-081763/200211
Related WPI Acc No: 2000-222210
XRPX Acc No: N02-060846
Protection system for programs and/or data involves encrypted data held in memory e.g. smart card, and unique key , encrypted **by** master **algorithm, held in another part of same memory**
Patent Assignee: ASHE V (ASHE-I)
Inventor: ASHE V
Number of Countries: 001 Number of Patents: 001
Patent Family:
Patent No Kind Date Applicat No Kind Date Week
US 6282651 B1 20010828 US 97896183 A 19970717 200211 B
US 99415189 A 19991007

Priority Applications (No Type Date): US 97896183 A 19970716; US 99415189 A 19991007

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6282651	B1		8	G06F-012/14	Div ex application US 97896183 Div ex patent US 6014745

Abstract (Basic): US 6282651 B1

NOVELTY - Memory e.g. smart card, holds data encrypted by algorithm unique to user in one part of memory and **encrypted key** in **another**. **Key encrypted** using **master** algorithm. Card put into Digital Signal Processor (DSP) device e.g. cash machine. User inserts **master key** (41) e.g. Personal Identification Number (PIN). Key on card decrypted using master algorithm (43). Compared to inserted PIN (45). If match, data decrypted (51).

DETAILED DESCRIPTION - Method may be used to protect data in other types of memory e.g. Electronically Programmable Read Only Memory (EPROM), masked Read Only Memory (ROM), compact disk (CD) or floppy disk which can be read using a processing unit e.g. DSP which contains the master algorithm.

USE - As a security system for protecting data held in a memory unit (claimed) e.g. EPROM, CD or smart card.

ADVANTAGE - Since data and key in memory are encrypted using different algorithms it cannot be deciphered without the master algorithm and **master key** e.g.(PIN).

DESCRIPTION OF **DRAWING** (S) - **Drawing** shows a flow chart of the data protection system applied to a smart card.

User inserts key (PIN) (41)

Key decrypted (43)

Inserted key compared to decrypted key (45)

Data decrypted (51)

pp; 8 DwgNo 4A/4

Title Terms: PROTECT; SYSTEM; PROGRAM; DATA; ENCRYPTION; DATA; HELD; MEMORY; SMART; CARD; UNIQUE; KEY; ENCRYPTION; MASTER; ALGORITHM; HELD; PART; MEMORY

Derwent Class: T01; W01

International Patent Class (Main): **G06F-012/14**

International Patent Class (Additional): **H04L-009/14** ; **H04L-009/32**

File Segment: EPI

30/5/17 (Item 11 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014191773 **Image available**

WPI Acc No: 2002-012470/200202

XRPX Acc No: N02-010297

Method of establishing secure communications link by encrypting user authorization information using shared **electronic** key

Patent Assignee: DEW ENG & DEV LTD (DEWE-N)

Inventor: HILLHOUSE R D

Number of Countries: 025 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1079565	A2	20010228	EP 2000118449	A	20000824	200202	B

Priority Applications (No Type Date): US 99382493 A 19990825

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1079565	A2	E	10	H04L-009/08	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Abstract (Basic): EP 1079565 A2

NOVELTY - Method consists in transmitting a first **public key** corresponding to the first **private key** from the first to the second

station, receiving it, along with user authorization information from the user of the second station, determining a **shared** electronic **key** from the first public and second **private keys** , or from the second **public key** corresponding to the first and **second private keys** , **encrypting** the user authorization information using the **shared key** , and transmitting the encrypted information and second **public key** from the second station to the first. These are **received** , the key is found from the second public and first **private keys** , user authorization information is decrypted and registered against stored data. If the user of the second station is authorized a secure communication session is initiated between the two stations.

USE - Method relates to cryptographic systems providing secure communications using an insecure network.

ADVANTAGE - Method uses authorization or biometric information to establish a secure communications link.

DESCRIPTION OF **DRAWING** (S) - The figure shows a flow chart of the method.

pp; 10 DwgNo 2/3

Title Terms: METHOD; ESTABLISH; SECURE; COMMUNICATE; LINK; USER; INFORMATION; SHARE; ELECTRONIC; KEY

Derwent Class: W01

International Patent Class (Main): **H04L-009/08**

International Patent Class (Additional): **H04L-009/32**

File Segment: EPI

30/5/18 (Item 12 from file: 350)

DIALOG(R)File 350:Derwent WPIX

013596527 **Image available**

WPI Acc No: 2001-080734/200109

XRPX Acc No: N01-061467

Configurable encryption/decryption method for multiple services support includes utilizing of common memory to encrypt first data stream **at** first **level of encryption and to second data stream at second level of encryption**

Patent Assignee: GEN INSTR CORP (GENN)

Inventor: QIU X; SPRUNK E J

Number of Countries: 094 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200077972	A1	20001221	WO 2000US15944	A	20000609	200109	B
AU 200054790	A	20010102	AU 200054790	A	20000609	200121	
EP 1198919	A1	20020424	EP 2000939752	A	20000609	200235	
			WO 2000US15944	A	20000609		

Priority Applications (No Type Date): US 2000587932 A 20000606; US 99138919 P 19990611

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200077972	A1	E	30	H04L-009/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW

AU 200054790	A		H04L-009/00	Based on patent WO 200077972
EP 1198919	A1	E	H04L-009/00	Based on patent WO 200077972

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Abstract (Basic): WO 200077972 A1

NOVELTY - Method includes storing a **first** set of **encryption key** associated with a **first data stream** . Encrypting a **first data stream** having **first** level of encryption, storing a second set

of encryption key associated with a second data stream. Encrypting the second data stream having a second level of encryption, utilizing a common memory to encrypt **first data stream** at **first** level of encryption and to encrypt second data stream at second level of encryption.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a cryptography circuit.

USE - Multiple services support such as cable company supply different services e.g. cable programs, subtitles, foreign language audio tracks, an internet connection, audio programs, pay-per-view channels, a programming guides etc. to different customers.

ADVANTAGE - It allows encryption system to provide several services encrypted at a low level of encryption while also providing a high level of encryption when only a few services are transmitted to a customer. The circuitry is configured so that the same circuitry or integrated circuit is utilized to accomplish both type of encryption.

DESCRIPTION OF DRAWING(S) - Drawing shows a flow chart illustrating the transmission and receipt, respectively, of two sets of services to a customer at different levels of encryption.

pp; 30 DwgNo 1/9

Title Terms: CONFIGURATION; ENCRYPTION; DECRYPTER; METHOD; MULTIPLE; SERVICE; SUPPORT; UTILISE; COMMON; MEMORY; FIRST; DATA; STREAM; FIRST; LEVEL; ENCRYPTION; SECOND; DATA; STREAM; SECOND; LEVEL; ENCRYPTION

Derwent Class: W01; W02

International Patent Class (Main): **H04L-009/00**

International Patent Class (Additional): H04N-007/167

File Segment: EPI

30/5/19 (Item 13 from file: 350)

DIALOG(R)File 350:Derwent WPIX

013111009 **Image available**

WPI Acc No: 2000-282880/200024

XRPX Acc No: N00-212921

Data communication method for password enhancing developed involves entering user password and irreversibly encrypting it using hash operation and public key encryption **algorithm**

Patent Assignee: COMODO TECHNOLOGY DEV LTD (COMO-N)

Inventor: ABDULHAYOGLU M

Number of Countries: 089 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200011537	A1	20000302	WO 99GB2672	A	19990812	200024	B
AU 9953811	A	20000314	AU 9953811	A	19990812	200031	
EP 1105784	A1	20010613	EP 99939542	A	19990812	200134	
			WO 99GB2672	A	19990812		
JP 2002523941	W	20020730	WO 99GB2672	A	19990812	200264	
			JP 2000566735	A	19990812		

Priority Applications (No Type Date): GB 9818186 A 19980820

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200011537	A1	E	27	G06F-001/00	

Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW

AU 9953811	A		G06F-001/00	Based on patent WO 200011537
EP 1105784	A1	E	G06F-001/00	Based on patent WO 200011537

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

JP 2002523941	W	23	H04L-009/32	Based on patent WO 200011537

Abstract (Basic): WO 200013437 A1

NOVELTY - Method enhances a password by irreversibly encrypting it after it is entered using a hash operation., and an additional step of using an **encrypted** stored **key** (NEPKEY) to **encrypt** the irreversibly encrypted user password (HASH), using a **public key encryption** algorithm. In an **additional** step an **encrypted second** stored **key** (UPEK) is decrypted using the decrypted first stored key (NEPKEY).

DETAILED DESCRIPTION - An independent claim describes a data communication system.

USE - As a method for password enhancing developed b entering a user password and irreversibly encrypting the user password.

ADVANTAGE - Provides for secure password handling by enhancing the password.

DESCRIPTION OF **DRAWING** (S) - The **drawing** shows a functional flow diagram illustrating the operation of the method.

pp; 27 DwgNo 2/4

Title Terms: DATA; COMMUNICATE; METHOD; PASSWORD; ENHANCE; DEVELOP; ENTER; USER; PASSWORD; IRREVERSIBLE; HASH; OPERATE; PUBLIC; KEY; ENCRYPTION; ALGORITHM

Derwent Class: T01

International Patent Class (Main): **G06F-001/00 ; H04L-009/32**

International Patent Class (Additional): **G06F-015/00 ; H04L-009/08**

File Segment: EPI

30/5/20 (Item 14 from file: 350)

DIALOG(R)File 350:Derwent WPIX

013097697 **Image available**

WPI Acc No: 2000-269569/200023

Related WPI Acc No: 1998-100585; 1998-286214

XRPX Acc No: N00-201743

Mobile satellite system e.g. for fraud detection and user validation system, requesting, by user, to become subscriber in communication system

Patent Assignee: SIGLER C E (SIGL-I); TISDALE W R (TISD-I)

Inventor: SIGLER C E; TISDALE W R

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6035039	A	20000307	US 95565036	A	19951130	200023	B
			US 9824256	A	19980217		

Priority Applications (No Type Date): US 95565036 A 19951130; US 9824256 A 19980217

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6035039	A		44	H04L-009/00	Div ex application US 95565036
					Div ex patent US 5748742

Abstract (Basic): US 6035039 A

NOVELTY - The method involves requesting, by a user, to become a subscriber in a communication system. A **first security key** is generated using a first **data** encryption **algorithm** having two input signals generated by respective two random number generating methods.

DETAILED DESCRIPTION - A second security key is generated using a second **data** encryption **algorithm** having third and fourth input signals, the third input signal includes the **first security key** and the fourth input signal includes data from one of the transmit and receive frequencies utilized by the mobile communication system. A verification is made so that the mobile communication system is authorized to utilize the communication system using the second security key. An INDEPENDENT CLAIM is included for a fraud prevention system.

USE - For fraud detection and user validation system.

ADVANTAGE - Detects presence of unauthorized **mobile telephone** in efficient manner.

DESCRIPTION OF DRAWING(S) - The figure shows a diagram illustrating an overview of the satellite network system.

pp; 44 DwgNo 1/35

Title Terms: MOBILE; SATELLITE; SYSTEM; FRAUD; DETECT; USER; VALID; SYSTEM; REQUEST; USER; SUBSCRIBER; COMMUNICATE; SYSTEM

Derwent Class: T01; W01; W02

International Patent Class (Main): **H04L-009/00**

International Patent Class (Additional): **G06F-007/04** ; G07D-007/00; H04K-001/00

File Segment: EPI

30/5/21 (Item 15 from file: 350)

DIALOG(R)File 350:Derwent WPIX

012960968 **Image available**

WPI Acc No: 2000-132818/200012

XRPX Acc No: N00-100579

Encryption and authentication system for use in providing communication security in communication network

Patent Assignee: TOYO COMMUNICATION EQUIP CO (TOCM)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2000004223	A	20000107	JP 98185610	A	1998061	200012	B

Priority Applications (No Type Date): JP 98185610 A 19980616

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2000004223	A		7	H04L-009/26	

Abstract (Basic): JP 2000004223 A

NOVELTY - The encryption sentence of a communication device is decoded by an encryption decoder (19) to **obtain** an n-bit **encryption key** . A dummy random-number series is **obtained** to input the n-bit **encryption key** in a dummy random-number generator (21). A decoding device (19) **obtains** a communication signal by performing OR operation of dummy random-number series and encryption sentence of the communication device.

DETAILED DESCRIPTION - The disclosure **key encryption** device (11) of an encryption apparatus (7) produces a predetermined **encryption key** by performing the encryption of **another encryption key** with the disclosure key, based on a **public - key** crypto system. A dummy random-number series is **obtained** to input the output value of the bits of an n-step linear feedback shift register into a bent function, and to input the n-bit **encryption key** of the communication signal into the dummy random-number generator. The encryption apparatus **obtains** the encryption sentence by applying the exclusive OR operation to the dummy random-number series and communication signal. The communication device performs the communication of the **encryption key** and the **encryption** sentence.

USE - For use in providing communication security in communication network.

ADVANTAGE - Improves safety of data communication in communication network. Ensures high-speed encryption and authentication system.

DESCRIPTION OF **DRAWING** (S) - The figure shows the block diagram of an encryption and authentication system.

Encryption apparatus (7)

Disclosure **key encryption** device (11)

Decoding device (19)

Encryption decoder (19)

Dummy random-number generator (21

Title Terms: ENCRYPTION; AUTHENTICITY; SYSTEM; COMMUNICATE; SECURE; COMMUNICATE; NETWORK

Derwent Class: P85; W01

International Patent Class (Main): **H04L-009/26**

International Patent Class (Additional): G09C-001/00; **H04L-009/32**
File Segment: EPI; EngPI

30/5/22 (Item 16 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012917558 **Image available**
WPI Acc No: 2000-089394/200008
XRPX Acc No: N00-070384

Method for enhancing security of broadcast program stored for subsequent use in subscriber terminal in a pay broadcasting system

Patent Assignee: MATSUSHITA ELECTRIC IND CO LTD (MATU); MATSUSHITA DENKI SANGYO KK (MATU)
Inventor: GOTO Y; HARADA T; KATAOKA M; MACHIDA K; MASUDA I
Number of Countries: 031 Number of Patents: 009
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 969667	A2	20000105	EP 99112808	A	19990702	200008 B
AU 9937949	A	20000120	AU 9937949	A	19990701	200015
JP 2000023137	A	20000121	JP 98201090	A	19980702	200015
SG 71930	A1	20000418	SG 993148	A	19990702	200027
CN 1249621	A	20000405	CN 99110174	A	19990702	200034
KR 2000011441	A	20000225	KR 9926613	A	19990702	200102
TW 416246	A	20001221	TW 99111202	A	19990701	200133
AU 741900	B	20011213	AU 9937949	A	19990701	200210
KR 304806	B	20011101	KR 9926613	A	19990702	200238

Priority Applications (No Type Date): JP 98201090 A 19980702
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 969667	A2	E	14	H04N-007/16	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
AU 9937949	A			H04L-009/16	
JP 2000023137	A		13	H04N-007/167	
SG 71930	A1			H04N-007/16	
CN 1249621	A			H04N-007/16	
KR 2000011441	A			H04N-007/167	
TW 416246	A			H04N-007/167	
AU 741900	B			H04L-009/16	Previous Publ. patent AU 9937949
KR 304806	B			H04N-007/167	Previous Publ. patent KR 2000011441

Abstract (Basic): EP 969667 A2

NOVELTY - Data of a broadcast program is scrambled with a scramble key updated in a short period. The scramble **key** is **encrypted** with a first key assigned to the subscriber terminal. The first **key** is **encrypted** with a first **master key** set in the subscriber terminal. A central station generates a **second key - encrypted** scramble **key** by **encrypting** the scramble **key** with a second key different from the first key and changeable in an interval shorter than a update interval of the first **key** , generates an **encrypted second key** by **encrypting** the **second key** with a second **master key** which has been commonly issued to subscriber terminals of the system, and broadcasts the **second key - encrypted** scramble **key** and the **encrypted second key** together with the scrambled data of the program, the first **key - encrypted** scramble **key** and the **encrypted** first **key** in a multiplexed manner.

DETAILED DESCRIPTION - When a broadcast program is to be stored, the subscriber terminal stores the scrambled data of the broadcast program and the **second key - encrypted** scramble **key** ; decrypt the **encrypted second key** with the second **master key** into the second key, which is added to a stored program second key list. If the stored program is to be executed, the **second key - encrypted** scramble **key** is decrypted with a corresponding one of the second keys in the stored program second key list into a decrypted scramble key. The scrambled data of the broadcast program is unscrambled with the

decrypted scramble key. INDEPENDENT CLAIMS are included for a station for broadcasting a program, and a subscriber terminal.

USE - For enhancing security of broadcast program stored for subsequent use in subscriber terminal in a pay broadcasting system.

ADVANTAGE - Provides enhanced security against illegal misuse.

DESCRIPTION OF **DRAWING** (S) - The figure shows a schematic block diagram of a subscriber terminal.

pp; 14 DwgNo 4/5

Title Terms: METHOD; ENHANCE; SECURE; BROADCAST; PROGRAM; STORAGE; SUBSEQUENT; SUBSCRIBER; TERMINAL; PAY; BROADCAST; SYSTEM

Derwent Class: W02

International Patent Class (Main): **H04L-009/16** ; H04N-007/16; H04N-007/167

International Patent Class (Additional): H04H-001/00; **H04L-009/08** ; **H04L-009/14**

File Segment: EPI

30/5/23 (Item 17 from file: 350)

DIALOG(R)File 350:Derwent WPIX

012703159

WPI Acc No: 1999-509268/199943

XRPX Acc No: N99-379495

Copy prevention apparatus for preventing copying of contents of recording medium e.g. floppy disk, compact disk CD, digital video disk DVD - has extraction circuit that obtains **watermark information from encrypted and then decoded multimedia data, and disk key acquisition unit that** obtains **disk key based on partial** master key

Patent Assignee: TOSHIBA KK (TOKE); TOSHIBA MICROELECTRONICS CORP (TOSZ)

Inventor: ENDOH K; ENDOH N; KATO T; YAMADA H

Number of Countries: 004 Number of Patents: 007

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
CN 1220459	A	19990623	CN 98122544	A	19981120	199943 B
JP 11232779	A	19990827	JP 98323879	A	19981113	199945
KR 99045452	A	19990625	KR 9849893	A	19981120	200036
US 6301663	B1	20011009	US 98195918	A	19981119	200162
US 20020003880	A1	20020110	US 98195918	A	19981119	200208
			US 2001934762	A	20010823	
KR 279523	B	20010302	KR 9849893	A	19981120	200214
US 6438692	B1	20020820	US 98195918	A	19981119	200257
			US 2001934762	A	20010823	

Priority Applications (No Type Date): JP 97361980 A 19971120

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
CN 1220459	A		1	G11B-020/10	
JP 11232779	A		20	G11B-020/10	
KR 99045452	A			G11B-020/10	
US 6301663	B1			H04L-009/00	
US 20020003880	A1			H04N-007/167	Div ex application US 98195918
					Div ex patent US 6301663
KR 279523	B			G11B-020/10	Previous Publ. patent KR 99045452
US 6438692	B1			H04L-009/32	Div ex application US 98195918
					Div ex patent US 6302663

Abstract (Basic): CN 1220459 A

NOVELTY - An extraction circuit (11) **obtains** the watermark information from the encrypted and then decoded multimedia data. A disk key acquisition unit **obtains** a disk key based on a partial **master key** . The **obtained** disk key is used in a fourth decoding unit for decoding multimedia transmitted by a fourth transmitter. DETAILED DESCRIPTION - An encryption circuit (4) has a first encryption unit that **encrypts** the disk **key** of a decoding circuit (5) which is connected to the encryption circuit via a CPU bus (B), using the disk

key itself. A first transmitter transmits the **encrypted** disk key. A **second encryption** unit **encrypts** the disk **key** using a **master key** . A second transmitter transmits the **encrypted** disk **key** . A third **encryption** unit encrypts multimedia data in which an electronic watermark information which is a part of the **master key** is embedded. A third transmitter transmits the encrypted multimedia data. A first and second decoding unit individually decodes the two **encrypted** disk **keys** . A third decoding unit decodes the encrypted multimedia data.

USE - For preventing copying contents of recording medium e.g. floppy disk, CD, DVD.

ADVANTAGE - Illegal selling of copies is prevented. Enables copyright to be protected more firmly. DESCRIPTION OF **DRAWING** (S) - The **drawing** shows the block diagram of the copy prevention apparatus. (4) Encryption circuit; (5) Decoding circuit; (11) Extraction circuit; (B) CPU bus.

JP 11232779 A

NOVELTY - An extraction circuit (11) **obtains** the watermark information from the encrypted and then decoded multimedia data. A disk key acquisition unit **obtains** a disk key based on a partial **master key** . The **obtained** disk key is used in a fourth decoding unit for decoding multimedia transmitted by a fourth transmitter. DETAILED DESCRIPTION - An encryption circuit (4) has a first encryption unit that **encrypts** the disk **key** of a decoding circuit (5) which is connected to the encryption circuit via a CPU bus (B), using the disk key itself. A first transmitter transmits the **encrypted** disk key. A **second encryption** unit **encrypts** the disk **key** using a **master key** . A second transmitter transmits the **encrypted** disk **key** . A third **encryption** unit encrypts multimedia data in which an electronic watermark information which is a part of the **master key** is embedded. A third transmitter transmits the encrypted multimedia data. A first and second decoding unit individually decodes the two **encrypted** disk **keys** . A third decoding unit decodes the encrypted multimedia data.

USE - For preventing copying contents of recording medium e.g. floppy disk, CD, DVD.

ADVANTAGE - Illegal selling of copies is prevented. Enables copyright to be protected more firmly. DESCRIPTION OF **DRAWING** (S) - The **drawing** shows the block diagram of the copy prevention apparatus. (4) Encryption circuit; (5) Decoding circuit; (11) Extraction circuit; (B) CPU bus.

Title Terms: COPY; PREVENT; APPARATUS; PREVENT; COPY; CONTENT; RECORD; MEDIUM; FLOPPY; DISC; COMPACT; DISC; CD; DIGITAL; VIDEO; DISC; EXTRACT; CIRCUIT; **OBTAIN** ; WATERMARK; INFORMATION; ENCRYPTION; DECODE; DATA; DISC ; KEY; ACQUIRE; UNIT; **OBTAIN** ; DISC; KEY; BASED; MASTER; KEY

Derwent Class: P85; T03; W04

International Patent Class (Main): G11B-020/10; **H04L-009/00** ; **H04L-009/32** ; H04N-007/167

International Patent Class (Additional): **G06F-012/14** ; G09C-001/00; G09C-005/00; G11B-007/00; **H04L-009/10**

File Segment: EPI; EngPI

30/5/24 (Item 18 from file: 350)

DIALOG(R)File 350:Derwent WPIX

012598500 **Image available**

WPI Acc No: 1999-404606/199934

XRPX Acc No: N99-301574

Transferring method of disk key and media key from media storage to output device in computer system

Patent Assignee: COMPAQ COMPUTER CORP (COPQ)

Inventor: ANGELO M F; DRISCOLL D J

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week

US 5923754 A 1999071[redacted] US 97850729 A 19970502 [redacted]9934 B

Priority Applications (No Type Date): US 97850729 A 19970502
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
US 5923754 A 7 H04L-009/00

Abstract (Basic): US 5923754 A

NOVELTY - A first random secure transfer key is generated with an uniqueness factor **derived** from a phase lock loop circuitry. A second transfer key is formed by combining the first key with an output device key. The second key is used to **encrypt** a disk **key** and a media key, so as to form a third secure transfer key.

DETAILED DESCRIPTION - The first secure transfer key is generated during power-ON state of a computer system. The first secure transfer key is deleted subsequently after the generation of **second** secure transfer **key** . The **encrypted** data **key** and media key are recovered from the third secure transfer key in the output device. An INDEPENDENT CLAIM is also included for the copy protection apparatus.

USE - For transferring disk key and media key from DVD disk, CD-ROM, magnetic tape, magnetic floppy disk to output device in computer system, for personal and commercial audio systems.

ADVANTAGE - Enables decrypting data only by using recipient's **private key** , since the knowledge of **key** used for **encryption** is insufficient to allow messages to be decrypted.

DESCRIPTION OF **DRAWING** (S) - The **drawing** shows the flowchart explaining negotiating of device keys during power-ON of computer system.

pp; 7 DwgNo 2/3

Title Terms: TRANSFER; METHOD; DISC; KEY; MEDIUM; KEY; MEDIUM; STORAGE; OUTPUT; DEVICE; COMPUTER; SYSTEM
Derwent Class: W01
International Patent Class (Main): **H04L-009/00**
File Segment: EPI

30/5/25 (Item 19 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012468161 **Image available**
WPI Acc No: 1999-274269/199923
XRPX Acc No: N99-205827

Encryption key **management procedure for data communication system - involves forwarding authentication data using** master **and additional** keys **which is then decoded to generate** additional encryption keys

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)
Number of Countries: 001 Number of Patents: 001
Patent Family:
Patent No Kind Date Applicat No Kind Date Week
JP 11088317 A 19990330 JP 97242975 A 19970908 199923 B

Priority Applications (No Type Date): JP 97242975 A 19970908
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
JP 11088317 A 11 H04L-009/08

Abstract (Basic): JP 11088317 A

NOVELTY - An additional key is generated using the **master key** and execution data. Then specific authentication data is generated by encrypting the data using **master** and additional **keys** . The authentication data is forwarded to the receiving side which is then decoded and **additional encryption key** is generated. The **received** message is decoded by **additional encryption key** . DETAILED DESCRIPTION - The user confidential data or **master key** and execution key are registered in key management unit. During communication, the encrypted data is transferred to the receiving side

user. A dummy key is generated using the dummy **master key** based on which confidential data is erased.

USE - For data communication system.

ADVANTAGE - The safety of data transmission is ensured irrespective of key management condition variation, thereby raises encryption efficiency. DESCRIPTION OF **DRAWING** (S) - The figure shows the block diagram of **encryption key** management system.

Dwg.1/7

Title Terms: ENCRYPTION; KEY; MANAGEMENT; PROCEDURE; DATA; COMMUNICATE; SYSTEM; FORWARDING; AUTHENTICITY; DATA; MASTER; ADD; KEY; DECODE; GENERATE; ADD; ENCRYPTION; KEY

Derwent Class: P85; W01

International Patent Class (Main): **H04L-009/08**

International Patent Class (Additional): G09C-001/00

File Segment: EPI; EngPI

30/5/26 (Item 20 from file: 350)

DIALOG(R)File 350:Derwent WPIX

012384218 **Image available**

WPI Acc No: 1999-190325/199916

XRPX Acc No: N99-139230

Encryption key **transfer system**

Patent Assignee: BARKAN M (BARK-I); DIVERSINET CORP (DIVE-N)

Inventor: BARKAN M

Number of Countries: 082 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9909700	A1	19990225	WO 98IL381	A	19980813	199916	B
AU 9886449	A	19990308	AU 9886449	A	19980813	199929	
EP 992139	A1	20000412	EP 98937753	A	19980813	200023	
			WO 98IL381	A	19980813		
IL 121551	A	20030410	IL 121551	A	19970814	200347	

Priority Applications (No Type Date): IL 121551 A 19970814

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9909700	A1	E	49	H04L-009/08	

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

AU 9886449	A		H04L-009/08	Based on patent WO 9909700
EP 992139	A1	E	H04L-009/08	Based on patent WO 9909700

Designated States (Regional): BE DE DK FR GB

IL 121551	A		H04L-009/08

Abstract (Basic): WO 9909700 A1

NOVELTY - System uses a center for secure distribution of **encryption keys** , certificates or permits to users at different locations. It enables change of the **public - private key** pair using means for storing the **encryption key** pair with two or more **additional encryption key** pairs, means for setting up a new key pair which comprises a new **private key** and the corresponding **public key** for the center, and means for preparing an announcement of the new **public key** for the center. The announcement includes copies of a message disclosing the new key, its number equaling the number of additional key pairs for reliable key dissemination. Each copy of the message is signed or encrypted with the pairs **private key** and the announcement is communicated to the parties.

USE - System is for reliable transfer of an **encryption key** .

ADVANTAGE - System provides recovery in case the **private key** is compromised and is more secure and flexible than systems using a single

encryption key .
DESCRIPTION OF **DRAWING** (S) - The figure shows
secret keys (SK)
public keys (PK)
key pair setting means (KIPS)
communication means (CM)
pp; 49 DwgNo 1/3
Title Terms: ENCRYPTION; KEY; TRANSFER; SYSTEM
Derwent Class: W01
International Patent Class (Main): **H04L-009/08**
International Patent Class (Additional): **H04L-009/16** ; **H04L-009/30**
File Segment: EPI

30/5/27 **(Item 21 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

012267083 **Image available**
WPI Acc No: 1999-073189/199907
XRPX Acc No: N99-053710
Key **recovery condition** encryption **apparatus e.g. for key recovery condition - has hashing unit calculating hash value on basis of hash function using key recovery information text as information necessary for performing key recovery**
Patent Assignee: FUJITSU LTD (FUIT); HITACHI LTD (HITA); NEC CORP (NIDE)
Inventor: ANDO H; DOMYO S; KANNO S; KURODA Y; MIYAUCHI H; MORITA I; SAKO K; TORII N; TSUCHIYA H; YAMAZAKI M
Number of Countries: 027 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 891053	A2	19990113	EP 98112477	A	19980706	199907	B
JP 11027254	A	19990129	JP 97181593	A	19970707	199915	
JP 3076273	B2	20000814	JP 97181593	A	19970707	200043	
US 6272225	B1	20010807	US 98110392	A	19980707	200147	

Priority Applications (No Type Date): JP 97181593 A 19970707
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 891053	A2	E	11	H04L-009/08	
	Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI				
JP 11027254	A		9	H04L-009/08	
JP 3076273	B2		8	H04L-009/08	Previous Publ. patent JP 11027254
US 6272225	B1			H04L-009/32	

Abstract (Basic): EP 891053 A
The apparatus comprises a hashing unit (100) to calculate a hash value on the basis of a hash function using a key recovery information text serving as information necessary for performing key recovery. A concatenating unit concatenates the hash value from the hashing unit to the key recovery condition. A condition information encryptor encrypts a concatenating result from the first concatenating unit by using an **encryption key** . The apparatus has a random generator (400) to generate an arbitrary random key serving as the first **encryption key** , a random **key encryptor** (310) **encrypts** the random **key** from the random generator by using a **private key** serving as a **second encryption key** , and a second concatenating unit concatenates an encryption result from the condition information encryptor to an encryption result from the random **key encryptor** .
The condition information encryptor encrypts the concatenating result from the first concatenating unit by using the random key from the random generator. The apparatus has an input to **receive** the key recovery information text and outputs the **received** key recovery information text to the hashing unit. A second input **receives** the key recovery condition and outputs the key recovery condition to the first

concatenating unit. A third input **receives** the **private key** and outputs the **private key** to the random **key encryptor** .

ADVANTAGE - Adds key recovery condition having relatively complex contents to key information without registering key recovery condition in third party organisation.

Dwg.1/4

Title Terms: KEY; RECOVER; CONDITION; ENCRYPTION; APPARATUS; KEY; RECOVER; CONDITION; HASH; UNIT; CALCULATE; HASH; VALUE; BASIS; HASH; FUNCTION; KEY ; RECOVER; INFORMATION; TEXT; INFORMATION; NECESSARY; PERFORMANCE; KEY; RECOVER

Derwent Class: P85; T01; W01

International Patent Class (Main): **H04L-009/08 ; H04L-009/32**

International Patent Class (Additional): G09C-001/00

File Segment: EPI; EngPI

30/5/28 (Item 22 from file: 350)

DIALOG(R)File 350:Derwent WPIX

012188654 **Image available**

WPI Acc No: 1998-605567/199851

XRPX Acc No: N98-472455

Key management method for encrypting message in communication system - involves generating session encryption key **to** encrypt **or decode data in calling side user apparatus and receiving side user apparatus, respectively**

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 10276184	A	19981013	JP 9777123	A	19970328	199851	B

Priority Applications (No Type Date): JP 9777123 A 19970328

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 10276184	A		9	H04L-009/08	

Abstract (Basic): JP 10276184 A

The method entails setting up a public system information and a secret and random system number at the time of system construction in a key management apparatus or a key registration apparatus. A user apparatus, the key registration apparatus, or the key management apparatus generates a public user information and confidential user information at the time of subscription by the user. The public system and user information are exhibited after a **master key** indicating a specific communication person is generated. The system number and confidential user information or the **master key** are registered to one or more key management systems.

When performing encryption, a calling side user apparatus generates a session **encryption key** . Additional data are added when the data contained in a session **key** are **encrypted** using the session **encryption key** . The additional data are transmitted to a receiving side user apparatus which generates **another** session **encryption key** . Another session key is produced when the additional data are decoded using the session **encryption key** .

ADVANTAGE - Unauthorised person cannot read message.

Dwg.1/6

Title Terms: KEY; MANAGEMENT; METHOD; MESSAGE; COMMUNICATE; SYSTEM; GENERATE; SESSION; ENCRYPTION; KEY; DECODE; DATA; CALL; SIDE; USER; APPARATUS; **RECEIVE** ; SIDE; USER; APPARATUS; RESPECTIVE

Derwent Class: W01

International Patent Class (Main): **H04L-009/08**

File Segment: EPI

30/5/29 (Item 23 from file: 350)

DIALOG(R)File 350:Derwent WPIX
(c) 2004 THOMSON DERWENT. All rts. reserv.

012030660 **Image available**
WPI Acc No: 1998-447570/199838
Related WPI Acc No: 1998-447415; 1998-447430
XRPX Acc No: N98-348863

Electronic network for transferring data units among storage elements - has information source with master and second encryption keys **with** encryption **engine for selectively encrypting data units using second key**

Patent Assignee: NORTON CO (NORT); CONNECTED CORP (CONN-N)
Inventor: CANE D; HIRSCHMAN D; SPEARE P; VAITZBLIT L
Number of Countries: 022 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9835472	A1	19980813	WO 98US2399	A	19980210	199838	B
AU 9864342	A	19980826	AU 9864342	A	19980210	199902	
NZ 507011	A	20030328	NZ 507011	A	19980210	200325	
			WO 99US2399	A	19980210		

Priority Applications (No Type Date): US 9814830 A 19980128; US 9737597 P 19970211
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9835472	A1	E	21	H04L-009/00	
	Designated States (National): AU CA JP NO NZ				
	Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE				
AU 9864342	A				Based on patent WO 9835472
NZ 507011	A			B24D-005/06	Based on patent WO 9835472

Abstract (Basic): WO 9835472 A

The electronic network includes a communications link. A source information processing system at a first end of the communications link includes a **master encryption key** , at least one secondary **encryption key** , a first memory which stores data units and the master and the at least one secondary **encryption key** and an **encryption** engine. The encryption engine selectively encrypts the data units to produce encrypted data units using at least one of the secondary **encryption keys** .

The encryption engine encrypts the secondary **encryption key** with the master **encryption key** to produce at least one **encrypted key** . An archive server information processing system at a second end of the communications link includes a second memory and is in communication with the source information processing system. The archive server information processing system **receives** and stores the encrypted data units and the **encrypted keys** in the second memory.

USE - For computer data backup system.

ADVANTAGE - Eliminates access to data by archive server. Provides source organisation with assurances of access control and privacy while relieving source organisation of archive cataloging and physical storage duties. Effective deletion of information stored on archive tapes is achieved without physical modification to magnetic tape.

Dwg.1/3

Title Terms: ELECTRONIC; NETWORK; TRANSFER; DATA; UNIT; STORAGE; ELEMENT; INFORMATION; SOURCE; MASTER; SECOND; ENCRYPTION; KEY; ENCRYPTION; ENGINE; SELECT; DATA; UNIT; SECOND; KEY
Derwent Class: P61; T01; W01
International Patent Class (Main): B24D-005/06; **H04L-009/00**
International Patent Class (Additional): B24D-003/08
File Segment: EPI; EngPI

30/5/30 (Item 24 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 THOMSON DERWENT. All rts. reserv.

011932261 **Image available**
WPI Acc No: 1998-349171/199831
XRPX Acc No: N98-272486

Cryptographic key managing method e.g. for two parties in communications networks - transporting, in different degrees of security **strength, symmetric** key encrypted **using asymmetric encryption technique and transporting ciphertext** derived **from plaintext** encrypted **under symmetric** key

Patent Assignee: NORTHERN TELECOM LTD (NELE); ENTRUST TECHNOLOGIES LTD (ENTR-N)
Inventor: VAN OORSCHOT P C; WIENER M J
Number of Countries: 002 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
CA 2213096	A	19980215	CA 2213096	A	19970814	199831	B
US 5850443	A	19981215	US 96698074	A	19960815	199906	
CA 2213096	C	20001031	CA 2213096	A	19970814	200060	

Priority Applications (No Type Date): US 96698074 A 19960815
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
CA 2213096	A		28	H04L-009/30	
US 5850443	A			H04L-009/08	
CA 2213096	C	E		H04L-009/30	

Abstract (Basic): CA 2213096 A

The method involves **encrypting** a cryptographic **key** of cryptographic strength commensurate with the degree of trust of the environment in which the party is located, by using a high trust **encryption public key** of the party to generate a party **encrypted** cryptographic **key** .

The cryptographic **key** is **encrypted** using a low trust **encryption public key** of the second party to generate a **second** party **encrypted** cryptographic **key** . The two parties **encrypted** cryptographic **keys** are concatentated. The second party, upon reception of the concatenated data is decrypted to recover the cryptographic key.

ADVANTAGE - Establishes **shared** secret cryptographic **keys** between two parties over communication network which spans both high-trust and low-trust environments. Ensures secure data transfer which originates in high-trust environment and for which intended recipients are either in high-trust environment or low-trust environment.

Dwg.1/4

Title Terms: CRYPTOGRAPHIC; KEY; MANAGE; METHOD; TWO; PARTY; COMMUNICATE; NETWORK; TRANSPORT; DEGREE; SECURE; STRENGTH; SYMMETRICAL; KEY; ENCRYPTION; ASYMMETRIC; ENCRYPTION; TECHNIQUE; TRANSPORT; DERIVATIVE; ENCRYPTION; SYMMETRICAL; KEY
Derwent Class: W01
International Patent Class (Main): **H04L-009/08 ; H04L-009/30**
International Patent Class (Additional): **H04L-009/00**
File Segment: EPI

30/5/31 (Item 25 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011869304 **Image available**
WPI Acc No: 1998-286214/199825
Related WPI Acc No: 1998-100585; 2000-269569
XRPX Acc No: N98-225023

Fraud detection and user validation system for mobile **earth** terminal **satellite communication - judges valid subscriber by subsequent authentication by comparing first and second components of respective security keys generated by central controller and mobile communication system**

Patent Assignee: AMSC SUBSIDIARY CORP (AMSC-N)
Inventor: SIGLER C E; TISDALE W R
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5748742	A	19980505	US 95565036	A	19951130	199825	B

Priority Applications (No Type Date): US 95565036 A 19951130
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5748742	A		61	H04L-009/00	

Abstract (Basic): US 5748742 A

The system includes a central controller which receives a first input signal from a mobile communication system. A **first security key** having a first component is generated by the central controller using a **data** encryption **algorithm** . Using the first input signal, a random number generator generates a second input signal in the central controller. A third input signal is generated in accordance to the receipt of the first input signal, by the central controller.

The third input signal is then transmitted to the mobile communication system. A second security key having a second component is generated in the mobile communication system using the **data** encryption **algorithm** . When communication is initiated, the mobile communication system verifies valid subscriber by subsequent authentication by comparing the first and second components of the respective security keys.

USE - For voice, data and facsimile transmission between mobile earth terminals and feeder link earth stations.

ADVANTAGE - Offers low cost, simple and reliable validation system. Enables easy rejection of unencrypted access. Identifies valid key stream reliably.

Dwg.1/35

Title Terms: FRAUD; DETECT; USER; VALID; SYSTEM; MOBILE; EARTH; TERMINAL; SATELLITE; COMMUNICATE; JUDGEMENT; VALID; SUBSCRIBER; SUBSEQUENT; AUTHENTICITY; COMPARE; FIRST; SECOND; COMPONENT; RESPECTIVE; SECURE; KEY; GENERATE; CENTRAL; CONTROL; MOBILE; COMMUNICATE; SYSTEM
Index Terms/Additional Words: MTS; MRS
Derwent Class: T01; W01; W02
International Patent Class (Main): **H04L-009/00**
International Patent Class (Additional): **G06F-007/04** ; G07D-007/00; H04K-001/00
File Segment: EPI

30/5/32 (Item 26 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011786034 **Image available**
WPI Acc No: 1998-202944/199818
XRPX Acc No: N98-161654

Software protective device e.g. for CPU control program - generates encrypted key based on predetermined encrypted key parameter, using which encrypted program which stipulates signal or information **processing** algorithm **is decoded**

Patent Assignee: MATSUSHITA DENKI SANGYO KK (MATU)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 10055273	A	19980224	JP 96313429	A	19961125	199818	B

Priority Applications (No Type Date): JP 96166841 A 19960605
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 10055273	A		15	G06F-009/06	

Abstract (Basic): JP 10055273 A

The device include[redacted] first encipherment unit (20) [redacted]h encodes an information transferred between CPU and memory via data bus. A **first encryption key** generator outputs an encrypted key, based on a predetermined encrypted key parameter. A first decoder decodes the encrypted information using the encrypted key.

A memory (24) is provided in which a program stipulating a signal processing or an **information** processing **algorithm** is encrypted and stored. The encrypted program is then decoded by a second decoder using a second encrypted key which in turn is output by a second encryption key generator, based on a predetermined encrypted key parameter.

ADVANTAGE - Improves software protectivity, efficiently.

Dwg.1/7

Title Terms: SOFTWARE; PROTECT; DEVICE; CPU; CONTROL; PROGRAM; GENERATE; ENCRYPTION; KEY; BASED; PREDETERMINED; ENCRYPTION; KEY; PARAMETER; ENCRYPTION; PROGRAM; SIGNAL; INFORMATION; PROCESS; ALGORITHM; DECODE

Derwent Class: P85; T01; W01

International Patent Class (Main): **G06F-009/06**

International Patent Class (Additional): **G06F-012/14** ; G09C-001/00; **H04L-009/16**

File Segment: EPI; EngPI

30/5/33 (Item 27 from file: 350)

DIALOG(R)File 350:Derwent WPIX

011582812 **Image available**

WPI Acc No: 1997-559293/199751

XRPX Acc No: N97-466115

Access key securing method e.g. for computer - creating two encrypted versions of access key first using key formed with user password and second formed using public key **from** public - private key **pair**

Patent Assignee: SYMANTEC CORP (SYMA-N)

Inventor: GRAWROCK D; LOHSTROH S R

Number of Countries: 020 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9742732	A1	19971113	WO 97US5964	A	19970410	199751	B
US 5768373	A	19980616	US 96643742	A	19960506	199831	
EP 894377	A1	19990203	EP 97920309	A	19970410	199910	
			WO 97US5964	A	19970410		

Priority Applications (No Type Date): US 96643742 A 19960506

Cited Patents: US 5436972; US 5481613; US 5557346; US 5557765; US 5633928; US 5640454

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9742732	A1	E	37	H04L-009/00	

Designated States (National): CA JP

Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE

EP 894377	A1	E		H04L-009/00	Based on patent WO 9742732

Designated States (Regional): DE FR GB

US 5768373	A			H04L-009/08	

Abstract (Basic): WO 9742732 A

The method involves **encrypting** an access **key** (232) with a first encryption algorithm to form a first encrypted version (236). The access **key** is **encrypted** with a second, asymmetric encryption algorithm to form a second encrypted version of the access **key** (270). A **public key** (266) from a **public - private key** pair is **obtained** for the **second encrypted** access **key** version.

Preferably, the first encrypted version of the access key is decrypted with a decryption algorithm. The second encrypted version of the access key is decrypted with an asymmetric decryption algorithm using a **private key** from a **public - private key** pair.

ADVANTAGE - Allows computer access even when forgotten password.

Allows to override password protection to data without significantly compromising data security.

Dwg.2/4

Title Terms: ACCESS; KEY; SECURE; METHOD; COMPUTER; TWO; ENCRYPTION; VERSION; ACCESS; KEY; FIRST; KEY; FORMING; USER; PASSWORD; SECOND; FORMING; PUBLIC; KEY; PUBLIC; PRIVATE; KEY; PAIR

Derwent Class: T01; W01

International Patent Class (Main): **H04L-009/00 ; H04L-009/08**

File Segment: EPI

30/5/34 (Item 28 from file: 350)

DIALOG(R)File 350:Derwent WPIX

011087735 **Image available**

WPI Acc No: 1997-065659/199706

XRPX Acc No: N97-053986

Secure communication method with cross-linked cryptographic codes - uses secure header message to identify operations centre and authenticate cryptographic control unit before communication of secure requests or usage reports to which operations centre responds

Patent Assignee: WAVE SYSTEMS CORP (WAVE-N)

Inventor: KAZMIERCZAK G J; MICHENER J R

Number of Countries: 025 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9642154	A1	19961227	WO 96US9382	A	19960606	199706	B
AU 9666739	A	19970109	AU 9666739	A	19960606	199717	
US 5671283	A	19970923	US 95488624	A	19950608	199744	
EP 836775	A1	19980422	EP 96926691	A	19960606	199820	
			WO 96US9382	A	19960606		

Priority Applications (No Type Date): US 95488624 A 19950608

Cited Patents: US 4078152; US 4229818; US 4264782; US 4933969

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9642154	A1	E	53	H04L-009/00	
Designated States (National): AU CA CN JP KR MX NO					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
AU 9666739	A			H04L-009/00	Based on patent WO 9642154
US 5671283	A		28	H04L-009/00	
EP 836775	A1	E		H04L-009/00	Based on patent WO 9642154
Designated States (Regional): DE FR GB IT					

Abstract (Basic): WO 9642154 A

The cryptographic communication method involves encrypting a message under a **first** cryptographic code **key** , using a **cipher** block chaining mode which has a first initial vector input, to form two encrypted data blocks. The encrypted data blocks are encrypted under a second cryptographic code key using the cipher block chaining mode with a second initial vector input for the first packet to form the first authentication code. The first authentication code is appended to the encrypted data blocks.

The second encrypted data blocks are encrypted under the second cryptographic code key using the cipher block chaining mode having a third initial vector input for the second packet to form the second message authentication code. One of the **first** encrypted **data blocks** of the **first** packet is selected as the third initial vector. The second authentication code is appended to the second encrypted data blocks. The message is sent to the receiving terminal where it is encrypted under the second cryptographic code key using the cipher block chaining mode and the third vector input. A second message authentication code is calculated. One of the encrypted **data blocks** of the **first** packet is selected as the third vector input.

USE/ADVANTAGE - Provides mechanism to allow remote cryptographic

control unit in user terminal and cryptographic operations centre to accurately authenticate and cross check message. Protects against reordering of packets within message.

Dwg.2/16

Title Terms: SECURE; COMMUNICATE; METHOD; CROSS; LINK; CRYPTOGRAPHIC; CODE; SECURE; HEADER; MESSAGE; IDENTIFY; OPERATE; CENTRE; AUTHENTICITY; CRYPTOGRAPHIC; CONTROL; UNIT; COMMUNICATE; SECURE; REQUEST; REPORT; OPERATE; CENTRE; RESPOND

Derwent Class: W01

International Patent Class (Main): **H04L-009/00**

International Patent Class (Additional): **H04L-009/06**

File Segment: EPI

30/5/35 (Item 29 from file: 350)

DIALOG(R)File 350:Derwent WPIX

010936368 **Image available**

WPI Acc No: 1996-433318/199643

Related WPI Acc No: 1998-286211; 1999-023867

XRPX Acc No: N96-365169

Secured communication encryption system with users being associated with public and private encryption keys **- generating** second **user session** encryption key **by** encrypting **session** key **with combination with** public encryption key **and central authority key**

Patent Assignee: BELL ATLANTIC NETWORK SERVICES (BELL-N)

Inventor: GANESAN R

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5557678	A	19960917	US 94277376	A	19940718	199643	B

Priority Applications (No Type Date): US 94277376 A 19940718

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5557678	A		13	H04L-009/16	

Abstract (Basic): US 5557678 A

The method involves generating a first user session **encryption key** by **encrypting** a session **key** with a combination of the **public encryption key** and the central authority key portion associated with a first user. A **second** user session **encryption key** is generated by **encrypting** a session **key** with a combination of the **public encryption key** and the central authority key portion associated with a second user. The first user session **encryption key** is decrypted by applying the **private** user **key** portion of the first user to **obtain** a common session **encryption key** available to the first user.

The method also entails decrypting the **second** user session **encryption key** by applying the **private** user **key** portion of the second user to **obtain** the common session **encryption key** available to the second user. The common session **encryption key** is used for encrypting and decrypting a first message exchanged during the session.

USE/ADVANTAGE - In split **private key** crypto-system for session key distribution. Facilitates confirmation of user's authorised access to another user of system by central intermediary each time communication system is initiated.

Dwg.2/5

Title Terms: SECURE; COMMUNICATE; ENCRYPTION; SYSTEM; USER; ASSOCIATE; PUBLIC; PRIVATE; ENCRYPTION; KEY; GENERATE; SECOND; USER; SESSION; ENCRYPTION; KEY; SESSION; KEY; COMBINATION; PUBLIC; ENCRYPTION; KEY; CENTRAL; AUTHORISE; KEY

Derwent Class: W01

International Patent Class (Main): **H04L-009/16**

International Patent Class (Additional): **H04L-009/30**

File Segment: EPI

30/5/36 (Item 30 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 THOMSON DERWENT. All rts. reserv.

010889551 **Image available**
WPI Acc No: 1996-386502/199639
XRPX Acc No: N96-325733

Printed document validation system with image information and data - receives document identification data and parts of encoded data from first processor and accesses associated image data in memory, forms second processor encoded data, compares data and produces validation signal if coincidence exists

Patent Assignee: EASTMAN KODAK CO (EAST)
Inventor: ELLSON R N; RAY L A
Number of Countries: 008 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 729120	A2	19960828	EP 96102382	A	19960216	199639	B
ZA 9509493	A	19960925	ZA 959493	A	19951108	199643	
JP 8305857	A	19961122	JP 9628177	A	19960215	199706	
EP 729120	A3	19961227	EP 96102382	A	19960216	199710	
US 5673320	A	19970930	US 95392713	A	19950223	199745	
BR 9600771	A	19971223	BR 96771	A	19960216	199806	
CN 1141456	A	19970129	CN 96103548	A	19960217	200051	

Priority Applications (No Type Date): US 95392713 A 19950223
Cited Patents: No-SR.Pub; EP 268450; EP 334616; EP 609937; US 5321751; WO 9203804
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 729120	A2	E	12	G07D-007/00	
Designated States (Regional): DE FR GB					
ZA 9509493	A		30	G06K-000/00	
JP 8305857	A		8	G06T-007/00	
EP 729120	A3			G07D-007/00	
US 5673320	A		10	H04L-009/00	
BR 9600771	A			G06K-009/62	
CN 1141456	A			G06K-009/00	

Abstract (Basic): EP 729120 A

The validation system includes several printed documents (12 and 10) each having data recorded on them representing the image of the authorised user and document identification data. The data is read (22). A non reversible encryption algorithm for encoding parts of the data is provided. A processor (26) encodes the read **data** with the **algorithm** (32). The image (28) of the user is displayed (30). A memory store has data corresp. to the image data stored in it.

A second processor (34) receives the document identification data and parts of the encoded data form the first processor, and accesses the associated image data from memory. The second processor processes the associated image data and parts of the received data to form **second** processor encoded **data** . **Parts** of the received encoded data is compared with the second processor encoded data to provide a validation signal if a correspondence is detected.

USE - For validating image data representing authorised user of several documents e.g. for signature, fingerprint or photographic data, where image data and document identification data is read and encoded for comparison against previously stored image data.

Dwg.2/4

Title Terms: PRINT; DOCUMENT; VALID; SYSTEM; IMAGE; INFORMATION; DATA; RECEIVE; DOCUMENT; IDENTIFY; DATA; PART; ENCODE; DATA; FIRST; PROCESSOR; ACCESS; ASSOCIATE; IMAGE; DATA; MEMORY; FORM; SECOND; PROCESSOR; ENCODE; DATA; COMPARE; DATA; PRODUCE; VALID; SIGNAL; COINCIDE; EXIST
Derwent Class: P31; T01; T05
International Patent Class (Main): G06K-000/00; G06K-009/00; G06K-009/62;

G06T-007/00; G07D-007/00; **H04L-009/00**
International Patent Class (Additional): A61B-005/117; G07F-007/12
File Segment: EPI; EngPI

30/5/37 (Item 31 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010642987 **Image available**
WPI Acc No: 1996-139941/199614
Related WPI Acc No: 2001-549122
XRPX Acc No: N96-117195
Key escrow and data escrow encryption - storing only public **escrow** keys **in sender and** receiver **and generating law enforcement access fields or data recovery fields**
Patent Assignee: TRUSTED INFORMATION SYSTEMS INC (TRUS-N); NETWORK ASSOC INC (NETW-N)
Inventor: BALENSON D M; ELLISON C M; LIPNER S B; WALKER S T
Number of Countries: 066 Number of Patents: 014
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9605673	A1	19960222	WO 95US10221	A	19950811	199614	B
AU 9533217	A	19960307	AU 9533217	A	19950811	199624	
US 5557346	A	19960917	US 94289602	A	19940811	199643	
US 5557765	A	19960917	US 94289602	A	19940811	199643	
			US 95390959	A	19950221		
EP 775401	A1	19970528	EP 95929479	A	19950811	199726	
			WO 95US10221	A	19950811		
US 5640454	A	19970617	US 94289602	A	19940811	199730	
			US 96715377	A	19960912		
US 5745573	A	19980428	US 94289602	A	19940811	199824	
			US 95390959	A	19950221		
			US 96691564	A	19960826		
			US 97781626	A	19970110		
KR 97705265	A	19970906	WO 95US10221	A	19950811	199839	
			KR 97700880	A	19970211		
JP 10508438	W	19980818	WO 95US10221	A	19950811	199843	
			JP 96507517	A	19950811		
BR 9508548	A	19981103	BR 958548	A	19950811	199849	
			WO 95US10221	A	19950811		
US 5956403	A	19990921	US 94289602	A	19940811	199945	
			US 96715377	A	19960912		
			US 97874459	A	19970616		
US 5991406	A	19991123	US 94289602	A	19940811	200002	
			US 95390959	A	19950221		
			US 96691564	A	19960802		
			US 97781626	A	19970110		
			US 9862748	A	19980420		
MX 9700980	A1	19980501	MX 97980	A	19970207	200007	
CN 1158195	A	19970827	CN 95195035	A	19950811	200140	

Priority Applications (No Type Date): US 95390959 A 19950221; US 94289602 A 19940811; US 96715377 A 19960912; US 96691564 A 19960826; US 97781626 A 19970110; US 97874459 A 19970616; US 9862748 A 19980420
Cited Patents: 02Jnl.Ref; EP 493232; WO 9321708
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9605673	A1	E	93	H04L-009/08	

Designated States (National): AM AT AU BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TT UA UZ VN
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT KE LU MC MW NL OA PT SD SE SZ UG

AU 9533217	A			H04L-009/08	Based on patent WO 9605673
US 5557346	A		28	H04L-009/08	
US 5557765	A		43	H04L-009/08	CIP of application US 94289602
EP 775401	A1	E		H04L-009/08	Based on patent WO 9605673

Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

US 5640454	A	28	H04L-009/08	Cont of application US 94289602 Cont of patent US 5557346
US 5745573	A	41	H04L-009/08	CIP of application US 94289602 Div ex application US 95390959 Cont of application US 96691564 CIP of patent US 5557346 Div ex patent US 5557765
KR 97705265	A		H04L-009/08	Based on patent WO 9605673
JP 10508438	W	121	H04L-009/08	Based on patent WO 9605673
BR 9508548	A		H04L-009/08	Based on patent WO 9605673
US 5956403	A		H04L-009/00	Cont of application US 94289602 Cont of application US 96715377 Cont of patent US 5557346 Cont of patent US 5640454
US 5991406	A		H04L-009/00	CIP of application US 94289602 Div ex application US 95390959 Cont of application US 96691564 Cont of application US 97781626 CIP of patent US 5557346 Div ex patent US 5557765 Cont of patent US 5745573
MX 9700980	A1		H04L-009/08	
CN 1158195	A		H04L-009/08	

Abstract (Basic): WO 9605673 A

The method for controlling an emergency decrypting user's access to a secret encrypted by a file encrypting user in a data recovery field (DRF), where the access to the message is controlled by an access rule (AR) defined by a rule defining user involves the AR defining user defines an access rule to control access to the secret and sends the AR to a data recovery centre (DRC). The DRC returns the access rule index (ARI) corresp. to the AR to the AR defining user.

The file encrypting user retrieves the ARI and generates the DRF. The DRF has the ARI and the secret encrypted by a DRC **public key**. The emergency decrypting user sends the DRF to the DRC. The DRC presents a challenge to the emergency decrypting user with the AR corresp. to the ARI in the DRF. The DRC sends the secret to the emergency decrypting user if the emergency user meets the challenge of the DRC.

USE/ADVANTAGE - Prevents any party having modified hardware or software from communicating with unmodified equipment or preventing law enforcement from gaining authorised access to communication.

Dwg.19/31

Title Terms: KEY; ESCROW; DATA; ESCROW; ENCRYPTION; STORAGE; PUBLIC; ESCROW ; KEY; SEND; **RECEIVE** ; GENERATE; LAW; ACCESS; FIELD; DATA; RECOVER; FIELD

Derwent Class: P85; W01

International Patent Class (Main): **H04L-009/00** ; **H04L-009/08**

International Patent Class (Additional): G09C-001/00; **H04L-009/30** ; **H04L-009/32**

File Segment: EPI; EngPI

30/5/38 (Item 32 from file: 350)

DIALOG(R)File 350:Derwent WPIX

010592097 **Image available**

WPI Acc No: 1996-089050/199610

XRPX Acc No: N96-074587

Controlling access to electronically-defined information among several users using locker-key symmetric cryptography - accessing storage location, obtaining **encrypted first** key **and using** private **second** key **to decrypt and recover first key**

Patent Assignee: AMERICAN TELEPHONE & TELEGRAPH CO (AMTT); AT & T CORP

(AMTT); LUCENT TECHNOLOGIES INC (LUCE)
Inventor: HAAS Z; PAUL S
Number of Countries: 006 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 695997	A2	19960207	EP 95305031	A	19950719	199610	B
CA 2151851	A	19960202	CA 2151851	A	19950615	199620	
JP 8063436	A	19960308	JP 95212947	A	19950731	199620	
US 5719938	A	19980217	US 94284025	A	19940801	199814	
CA 2151851	C	19990518	CA 2151851	A	19950615	199938	
EP 695997	B1	20021016	EP 95305031	A	19950719	200276	
DE 69528557	E	20021121	DE 628557	A	19950719	200302	
			EP 95305031	A	19950719		

Priority Applications (No Type Date): US 94284025 A 19940801
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 695997	A2	E	12	G06F-012/14	
Designated States (Regional): DE FR GB					
CA 2151851	A			H04L-009/28	
JP 8063436	A		12	G06F-015/00	
US 5719938	A		11	H04L-009/08	
CA 2151851	C	E		H04L-009/28	
EP 695997	B1	E		G06F-012/14	
Designated States (Regional): DE FR GB					
DE 69528557	E			G06F-012/14	Based on patent EP 695997

Abstract (Basic): EP 695997 A

The method involves attaining access by the predetermined user to the unencrypted electronically-defined information. The stored **encrypted second key** is accessed from a network-connected apparatus of the predetermined user. The accessed **encrypted second key** is decrypted using the first key of the predetermined user at the apparatus of the predetermined user to recover the **second encryption key** .

The stored encrypted information from the network-connected apparatus of the predetermined user is accessed. The accessed encrypted information is decrypted using the recovered **second encryption key** to recover the electronically-defined information for examination of the recovered information by the predetermined user.

USE/ADVANTAGE - E.g. for electronic newspaper. Provides secure access to information accessible to be shared among dynamically changing set of authorised users on network having server.

Dwg.2/7

Title Terms: CONTROL; ACCESS; ELECTRONIC; DEFINE; INFORMATION; USER; LOCKER ; KEY; SYMMETRICAL; ACCESS; STORAGE; LOCATE; **OBTAIN** ; ENCRYPTION; FIRST; KEY; PRIVATE; SECOND; KEY; RECOVER; FIRST; KEY
Derwent Class: P85; T01
International Patent Class (Main): **G06F-012/14** ; **G06F-015/00** ; **H04L-009/08** ; **H04L-009/28**
International Patent Class (Additional): G09C-001/00; **H04L-009/00** ; **H04L-009/10** ; **H04L-009/12**
File Segment: EPI; EngPI

30/5/39 (Item 33 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010011507 **Image available**
WPI Acc No: 1994-279219/199434
XRPX Acc No: N94-220021

Hybrid encryption for protecting reusable software components - combining conventional or private key algorithm with public key algorithm

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: MOORE J W
Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5343527	A	19940830	US 93141735	A	19931027	199434	B

Priority Applications (No Type Date): US 93141735 A 19931027
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5343527	A		22	H04L-009/00	

Abstract (Basic): US 5343527 A

The method for reusing software components that maintains the integrity and authenticity of the software components involves generating a software component record by encrypting a plaintext representation of a software component using a first cryptographic algorithm using **first key** . The **encrypted** software component is hashed to generate a **hash digest** . The **hash digest** and the **first key** are **encrypted** using a second cryptographic algorithm with a second key.

The second cryptographic algorithm is of a public key type and the second key is the private key associated with at least one public key. The software component record consists of the encrypted software component, the encrypted **hash digest** , and the **encrypted first key** . The software component record is stored in a reuse library.

USE/ADVANTAGE - Protection against unauthorised modification of software. Notifies user if software has been modified in any way.

Dwg.6/10

Title Terms: HYBRID; ENCRYPTION; PROTECT; REUSE; SOFTWARE; COMPONENT; COMBINATION; CONVENTION; PRIVATE; KEY; ALGORITHM; PUBLIC; KEY; ALGORITHM
Derwent Class: T01; W01
International Patent Class (Main): **H04L-009/00**
File Segment: EPI

30/5/40 (Item 34 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009910246 **Image available**
WPI Acc No: 1994-177952/199422
XRPX Acc No: N94-140164

Secure document production and authentication method - including scanning document to produce digital signal which is compressed, encrypted and coded as a two-dimensional barcode

Patent Assignee: PITNEY BOWES INC (PITB)
Inventor: BERSON W
Number of Countries: 020 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 600646	A2	19940608	EP 93309236	A	19931119	199422	B
CA 2109554	A	19940521	CA 2109554	A	19931119	199430	
JP 7005809	A	19950110	JP 93315848	A	19931122	199511	
US 5388158	A	19950207	US 92979116	A	19921120	199512	
EP 600646	A3	19971105	EP 93309236	A	19931119	199814	
CA 2109554	C	19981027	CA 2109554	A	19931119	199902	
EP 600646	B1	20000920	EP 93309236	A	19931119	200047	
DE 69329447	E	20001026	DE 629447	A	19931119	200061	
			EP 93309236	A	19931119		

Priority Applications (No Type Date): US 92979116 A 19921120
Cited Patents: No-SR.Pub; EP 286378; EP 317229; EP 334616; US 4663622; US 4893338; US 5159635; US 5241600
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 600646	A2	E	7	G07F-007/12	
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE					
CA 2109554	A			G06K-009/36	
JP 7005809	A		6	G09C-005/00	

US 5388158 A 6 H04L-009/32
EP 600646 A3 G07F-007/12
CA 2109554 C G06K-009/36
EP 600646 B1 E G07F-007/12
Designated States (Regional): DE FR GB NL
DE 69329447 E G07F-007/12 Based on patent EP 600646

Abstract (Basic): EP 600646 A

The method involves scanning a document to produce a signal representative of an image of at least a portion of the document. A second signal is encrypted comprising a representation of the image and **derived** from the first signal. A coded representation of the second encrypted signal is incorporated with the document. The coded representation of the second signal is then read from the document.

The method further involves decoding the second signal and decrypting the decoded signal. The decrypted second signal is input to a display to display the representation of the image. Finally the document is compared with the displayed image to authenticate the document.

ADVANTAGE - Allows production of document secure against tampering and alteration and is easily applied to existing documents or those produced in predefined format.

Dwg.1/2

Title Terms: SECURE; DOCUMENT; PRODUCE; AUTHENTICITY; METHOD; SCAN; DOCUMENT; PRODUCE; DIGITAL; SIGNAL; COMPRESS; ENCRYPTION; CODE; TWO; DIMENSION
Derwent Class: P85; T05; W02
International Patent Class (Main): G06K-009/36; G07F-007/12; G09C-005/00; **H04L-009/32**
International Patent Class (Additional): G06K-007/10; G07D-007/00; **H04L-009/08** ; **H04L-009/28** ; **H04L-009/30** ; H04N-001/44
File Segment: EPI; EngPI

30/5/41 (Item 35 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 THOMSON DERWENT. All rts. reserv.

009180697 **Image available**
WPI Acc No: 1992-308132/199237
XRPX Acc No: N92-235907

Data processing system with communication nodes - has encryption device which encode data block which is then transmitted to other node to be received and decoded by decryption circuit

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC); IBM CORP (IBMC)
Inventor: JOHNSON D B; LE A V; MATYAS S M; PRYMAK R; WILKINS J D; MARTIN W C; ROHLAND W S
Number of Countries: 011 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5142578	A	19920825	US 91748407	A	19910822	199237	B
EP 529261	A2	19930303	EP 92111758	A	19920710	199309	
CA 2068488	A	19930223	CA 2068488	A	19920512	199319	
EP 529261	A3	19931118	EP 92111758	A	19920710	199512	
JP 7202878	A	19950804	JP 92208406	A	19920713	199540	
EP 529261	B1	19970212	EP 92111758	A	19920710	199712	
DE 69217428	E	19970327	DE 617428	A	19920710	199718	
			EP 92111758	A	19920710		
CA 2068488	C	19980519	CA 2068488	A	19920512	199831	

Priority Applications (No Type Date): US 91748407 A 19910822
Cited Patents: No-SR.Pub; 2.Jnl.Ref; EP 354770; EP 356065; JP 3128541; US 4924515; US 4941176
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5142578	A		25	H04L-009/30	
EP 529261	A2	E	35	H04L-009/08	

Designated States (Regional): CH DE FR GB IT LI NL SE
JP 7202878 A 21 H04L-009/06
EP 529261 B1 E 45 H04L-009/08
Designated States (Regional): CH DE FR GB IT LI NL SE
DE 69217428 E H04L-009/08 Based on patent EP 529261
CA 2068488 A G06F-013/38
EP 529261 A3 H04L-009/30
CA 2068488 C G06F-013/38

Abstract (Basic): US 5142578 A

The apparatus distributes an **initial Data Encryption Algorithm** (DEA) **key - encrypting key** to **encrypting** a **key** record using a public key algorithm and a public key belonging to the intended recipient of the key record. The apparatus recovers the distributed key-encrypting key by the recipient by decrypting the received key record using the same public key algorithm and private key associated with the public key and re-encrypting the key-encrypting key under a key formed by arithmetically combining the recipient's master key with a control vector contained in the control information of the received key record.

The type and usage attributes assigned by the originator of the key-encrypting key in the form of a control vector are cryptographically coupled to the key-encrypting key such that the recipient may only use the received key-encrypting key in a manner defined by the key originator.

ADVANTAGE - Enhances security.

Dwg.15/16

Title Terms: DATA; PROCESS; SYSTEM; COMMUNICATE; NODE; ENCRYPTION; DEVICE; ENCODE; DATA; BLOCK; TRANSMIT; NODE; RECEIVE; DECODE; DECRYPTER; CIRCUIT
Derwent Class: P85; W01
International Patent Class (Main): **G06F-013/38** ; **H04L-009/06** ; **H04L-009/08** ; **H04L-009/30**
International Patent Class (Additional): G09C-001/00; **H04L-009/14**
File Segment: EPI; EngPI

30/5/42 (Item 36 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009165420 **Image available**
WPI Acc No: 1992-292854/199236
XRPX Acc No: N92-224345

Reliable authentication of communication e.g. postal indicia - encrypting key shared with second party, transmitting to second party, e.g. mailer, for appending before transmission to third party, e.g. postal service

Patent Assignee: PITNEY BOWES INC (PITB); PASTOR J (PAST-I)
Inventor: PASTOR J
Number of Countries: 002 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
CA 2056935	A	19920618	CA 2056935	A	19911204	199236	B
US 5142577	A	19920825	US 90628820	A	19901217	199237	
CA 2056935	C	19960618	CA 2056935	A	19911204	199636	

Priority Applications (No Type Date): US 90628820 A 19901217
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
CA 2056935	A		31	H04K-001/00	
US 5142577	A		12	H04L-009/02	
CA 2056935	C			H04K-001/00	

Abstract (Basic): CA 2056935 A

A third party may validate that a communication is an authentic communication from a second parety sent with the authorisation of a first party. For example, the third party may be a postal service, the

second party may be a mailer, and the communication may be a postal indicia showing that a mail piece has been properly franked. The first party and the second party share an **encryption key**, or a series of keys. The first party also has a **second encryption key** which the third party has the ability to decrypted.

The first party **encrypts** a **key shared** with the second party with the first party's second key and transmits this to the second party. The second party then uses its copy of the **key** to **encrypt** information and appends its encrypted information to the message **received** from the first party and transmits all this to the third party. The third party may then decrypt the copy of the **key encrypted** by the first party and use this information to decrypt the information encrypted by the second party. The known technique of eliptical logarithms may be used to provide highly secure encryption of short messages. The second party may be a mailer and the apparatus of the subject invention may include a postage meter which prints the information transmitted to the third party, who may be a postal service, on a mail piece as a postal indicia.

ADVANTAGE - Postal service does not need to maintain large data bank of keys for each mailer.

Dwg.3/3

Title Terms: RELIABILITY; AUTHENTICITY; COMMUNICATE; POSTAL; INDICIA; KEY; SHARE; SECOND; PARTY; TRANSMIT; SECOND; PARTY; MAIL; TRANSMISSION; THIRD; PARTY; POSTAL; SERVICE

Derwent Class: W01

International Patent Class (Main): H04K-001/00; **H04L-009/02**

International Patent Class (Additional): **H04L-009/28**

File Segment: EPI

30/5/43 (Item 37 from file: 350)

DIALOG(R)File 350:Derwent WPIX

008475593 **Image available**

WPI Acc No: 1990-362593/199049

XRPX Acc No: N90-276654

Coded transmission equipment for public communication system - uses coding appts. at calling and called stations operating with agreed code and authentication arrangement for appropriate security level

Patent Assignee: SIEMENS AG (SIEI)

Inventor: MARKWITZ W

Number of Countries: 016 Number of Patents: 008

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 3919734	C	19901206	DE 3919734	A	19890616	199049	B
WO 9016124	A	19901227				199103	
EP 477180	A	19920401	EP 90905428	A	19900405	199214	
JP 4506137	W	19921022	JP 90505301	A	19900405	199249	
			WO 90DE270	A	19900405		
US 5216715	A	19930601	WO 90DE270	A	19900405	199323	
			US 91793426	A	19911212		
EP 477180	B1	19940824	EP 90905428	A	19900405	199433	
			WO 90DE270	A	19900405		
DE 59006915	G	19940929	DE 506915	A	19900405	199438	
			EP 90905428	A	19900405		
			WO 90DE270	A	19900405		
CA 2062751	C	20000808	CA 2062751	A	19900405	200051	
			WO 90DE270	A	19900405		

Priority Applications (No Type Date): DE 3919734 A 19890616

Cited Patents: EP 205095; EP 307627; EP 48903

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9016124	A				

Designated States (National): CA JP US

Designated States (Regional): AT BE CH DE DK ES FR GB IT LU NL SE

EP 477180 A 24
Designated States (Regional): CH DE DK FR GB LI NL SE
JP 4506137 W 7 H04L-009/06 Based on patent WO 9016124
US 5216715 A 9 H04L-009/02 Based on patent WO 9016124
EP 477180 B1 G 12 H04L-009/32 Based on patent WO 9016124
Designated States (Regional): CH DE DK FR GB LI NL SE
DE 59006915 G H04L-009/32 Based on patent EP 477180
Based on patent WO 9016124
CA 2062751 C E H04K-001/00 Based on patent WO 9016124
Abstract (Basic): DE 3919734 C

The arrangement for transmitting codes is intended for a number of subscriber stations (TLN A,TLN,B),where a code is accep.ted for communication between sending and receiving stations. Coding equipment for the agreed code is provided in the stations which are given a recognition code. The communication system is equipped with an arrangement for authenticating a subscriber in the coded transmissions.

Depending on the desired degree of security in any transmission, the arrangement can adopt an appropriate checking response. There are two stages or grades of security. The first is intended for speech transmissions and employs a reduced scheme, while the second is more complicated and uses a central station (SMZ) for checking purposes.

USE/ADVANTAGE - Improvement is security for subscriber without undue expense. Suitable for data processing systems. (9pp Dwg.No.2/5)

Title Terms: CODE; TRANSMISSION; EQUIPMENT; PUBLIC; COMMUNICATE; SYSTEM; CODE; APPARATUS; CALL; CALL; STATION; OPERATE; AGREE; CODE; AUTHENTICITY; ARRANGE; APPROPRIATE; SECURE; LEVEL
Derwent Class: W01; W02
International Patent Class (Main): H04K-001/00; **H04L-009/02** ; **H04L-009/06** ; **H04L-009/32**
International Patent Class (Additional): H04B-007/26; **H04L-009/08** ; **H04L-009/14** ; **H04L-012/22** ; H04Q-007/02
File Segment: EPI

30/5/44 (Item 38 from file: 350)
DIALOG(R)File 350:Derwent WPIX

008382533 **Image available**
WPI Acc No: 1990-269534/199036
XRPX Acc No: N90-208616
Cipher key distribution system - stores public information on common file and has two sub-systems with transmitters and receivers
Patent Assignee: NEC CORP (NIDE)
Inventor: TANAKA K
Number of Countries: 008 Number of Patents: 009
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 385511	A	19900905	EP 90104200	A	19900305	199036	B
AU 9050706	A	19900906				199043	
CA 2011396	A	19900903				199047	
JP 3016339	A	19910124	JP 9050939	A	19900302	199110	
US 5029208	A	19910702	US 90488952	A	19900305	199129	
EP 385511	A3	19920603	EP 90104200	A	19900305	199332	
CA 2011396	C	19950103	CA 2011396	A	19900302	199510	
EP 385511	B1	19970806	EP 90104200	A	19900305	199736	
DE 69031185	E	19970911	DE 631185	A	19900305	199742	
			EP 90104200	A	19900305		

Priority Applications (No Type Date): JP 8980501 A 19890330; JP 8952352 A 19890303; JP 8952353 A 19890303; JP 8952354 A 19890303; JP 9050939 A 19900302
Cited Patents: NoSR.Pub; 1.Jnl.Ref; EP 257585
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 385511	A				

Designated States (Regional): DE FR GB NL

EP 385511 B1 E 23 H04L-009/08
Designated States (Regional): DE FR GB NL
DE 69031185 E H04L-009/08 Based on patent EP 385511
CA 2011396 C H04L-009/08

Abstract (Basic): EP 385511 A

A system includes a common file for storing public information in a position indicated by the receiving party identifying information. A transmitting subsystem is capable of reading the common file, generating random numbers and a cipher key, and storing secret information. The subsystem also generates a key distribution code and transmits this code together with **information identifying** the communicating party.

A receiving subsystem receives the key distributing code and identifies information, stores a constant and secret information and generates the same cipher key as the transmitting subsystem.

USE/ADVANTAGE - For one way communication system. Avoids excessive overheads and improves security.

Dwg.2/11

Title Terms: CIPHER; KEY; DISTRIBUTE; SYSTEM; STORAGE; PUBLIC; INFORMATION; COMMON; FILE; TWO; SUB; SYSTEM; TRANSMIT; RECEIVE
Derwent Class: P85; W01
International Patent Class (Main): **H04L-009/08**
International Patent Class (Additional): G09C-001/00; H04K-001/00
File Segment: EPI; EngPI

30/5/45 (Item 39 from file: 350)
DIALOG(R)File 350:Derwent WPIX

007929981
WPI Acc No: 1989-195093/198927
Related WPI Acc No: 1989-193738; 1989-195094
XRPX Acc No: N89-149165

Authentication of number of documents - providing decryption key for use with information provided by mailer

Patent Assignee: PITNEY BOWES INC (PITB)
Inventor: PASTOR J
Number of Countries: 009 Number of Patents: 012
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2211643	A	19890705	GB 8828987	A	19881212	198927	B
DE 3841389	A	19890713	DE 3841389	A	19881208	198929	
FR 2625636	A	19890707				198933	
AU 8825134	A	19890706				198934	
SE 8804236	A	19890807				198945	
US 4893338	A	19900109	US 87140051	A	19871231	199010	
CH 679346	A	19920131				199208	
SE 466678	B	19920316				199214	
GB 2211643	B	19920429	GB 8828987	A	19881212	199218	
IT 1224805	B	19901024	IT 8848634	A	19881209	199223	
CA 1331641	C	19940823	CA 583793	A	19881122	199435	
DE 3841389	C2	19970925	DE 3841389	A	19881208	199742	

Priority Applications (No Type Date): US 87140051 A 19871231; US 87136251 A 19871218
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2211643	A		26		
US 4893338	A		8		
DE 3841389	C2		9	H04L-009/32	
IT 1224805	B			G06F	
CA 1331641	C			H04L-009/00	

Abstract (Basic): GB 2211643 A

The system for conveying information for the reliable

authentication of number of documents (e.g. mail) includes a device for solving a set of polynomial equations to develop a string of characters and having a decryption key that, upon application to the string of characters, reveals not only a plain text message indicating the source of the authentication but, in addition, provides the decryption key for use with the information provided by the mailer. The solution of the set of polynomial equations requires the accumulation of individual documents, each having a random x, and the value f (x,) of the polynomial associated withit.

ADVANTAGE - Increased speed and efficiency.

3/3

Title Terms: AUTHENTICITY; NUMBER; DOCUMENT; DECRYPTER; KEY; INFORMATION; MAIL

Derwent Class: P85; T01; T04; T05

International Patent Class (Main): **G06F-307/00** ; **H04L-009/00** ; **H04L-009/32**

International Patent Class (Additional): G06K-005/00; G07D-007/00; G09C-001/00; G09C-005/00; H04K-001/00; **H04L-009/30**

File Segment: EPI; EngPI

30/5/46 (Item 40 from file: 350)

DIALOG(R)File 350:Derwent WPIX

007928626

WPI Acc No: 1989-193738/198927

Related WPI Acc No: 1989-195093; 1989-195094

XRPX Acc No: N89-148180

Public key encryption **system for third party documents - issues clear text indication of authorised originator and decryption key for information delivered by franking machine**

Patent Assignee: PITNEY BOWES INC (PITB)

Inventor: PASTOR J

Number of Countries: 009 Number of Patents: 011

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 3841393	A	19890629	DE 3841393	A	19881208	198927	B
FR 2625013	A	19890625				198932	
AU 8824760	A	19890622				198933	
SE 8804068	A	19890619				198937	
US 4853961	A	19890801	US 87136251	A	19871218	198938	
CH 679255	A	19920115				199208	
IT 1224787	B	19901024	IT 8848604	A	19881129	199240	
SE 468654	B	19930222	SE 884068	A	19881110	199310	
CA 1331640	C	19940823	CA 582676	A	19881108	199435	
DE 3841393	C2	19980219	DE 3841393	A	19881208	199811	
JP 3020958	B2	20000315	JP 88306778	A	19881203	200018	

Priority Applications (No Type Date): US 87136251 A 19871218; US 87140051 A 19871231

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 3841393	A		9		
JP 3020958	B2		9	H04L-009/32	Previous Publ. patent JP 1191891
US 4853961	A		8		
DE 3841393	C2		9	H04L-009/32	
IT 1224787	B			G06F	
SE 468654	B			G07D-007/00	
CA 1331640	C			H04L-009/08	

Abstract (Basic): DE 3841393 A

At the authorised originating station (30) a **public key** generator (32) and a processor (34) are associated with nonvolatile and real-time memories (36, 38) and a communication interface (e.g. microcomputer card) (40), linked (54) to an addressing and franking machine (42). This includes an encryption module (46) and nonvolatile

memory (48) in which the associated **public key** is stored.

The prepd. mail is delivered to an authorised post office (44) where a decryption module (56) operates with a keyboard or optical reader (58), and a communication interface (64) to the originating station (30). Document authenticity is indicated visually or audibly (62).

USE/ADVANTAGE - For verification of authenticity of paper documents or magnetic or optical discs. Does not require data-base large enough for decryption of all possible keys form different franking machines

Title Terms: PUBLIC; KEY; ENCRYPTION; SYSTEM; THIRD; PARTY; DOCUMENT; ISSUE ; CLEAR; TEXT; INDICATE; AUTHORISE; DECRYPTER; KEY; INFORMATION; DELIVER; FRANKING; MACHINE

Derwent Class: P85; T01; T04; T05

International Patent Class (Main): **G06F-001/68** ; G07D-007/00; **H04L-009/08** ; **H04L-009/32**

International Patent Class (Additional): G06K-005/00; G07B-017/00; G09C-001/00; G09C-001/10; G09C-005/00; **H04L-009/00** ; **H04L-009/30**

File Segment: EPI; EngPI

30/5/47 (Item 41 from file: 350)

DIALOG(R)File 350:Derwent WPIX

004611196

WPI Acc No: 1986-114540/198618

XRPX Acc No: N86-084363

Cryptographic system for direct broadcast satellite network - has data stream with encrypted **common** key **decrypted using signature key generated from secret** master key

Patent Assignee: GEN INSTR CORP (GENN)

Inventor: HORNE D

Number of Countries: 012 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 179612	A	19860430	EP 85307456	A	19851016	198618	B
JP 61107376	A	19860526	JP 85236525	A	19851024	198627	
CA 1244090	A	19881101				198848	
US 4887296	A	19891212	US 87113333	A	19871016	199007	
EP 179612	B	19910807				199132	
DE 3583722	G	19910912				199138	

Priority Applications (No Type Date): US 84665114 A 19841026

Cited Patents: A3...8725; EP 127381; EP 132401; GB 2124856; No-SR.Pub; US 4323921

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 179612	A	E	41		
Designated States (Regional): BE CH DE FR GB IT LI NL SE					
EP 179612	B				
Designated States (Regional): BE CH DE FR GB IT LI NL SE					

Abstract (Basic): EP 179612 A

Each of several **receiver** nodes has a unique address number, and a circuit (14) generates a common key. A circuit (12) encrypts the information to be distributed using the common key. A different individual key is generated for each **receiver** node, using a **master key** (20) and a circuit (22) using the Data Encryption Standard algorithm for **encrypting** the common **key** using the generated individual key for that **receiver** node.

The encrypted information is distributed to all **receiver** nodes and the individualised **encrypted** common **key** for each node is distributed to that **receiver** node.

ADVANTAGE - Only single **master key** must be stored and protected.

Title Terms: CRYPTOGRAPHIC; SYSTEM; DIRECT; BROADCAST; SATELLITE; NETWORK;

DATA; STREAM; ENCRYPTION; COMMON; KEY; SIGNATURE; KEY; GENERATE; SECRET; MASTER; KEY
Index Terms/Additional Words: SUBSCRIBER; TELEVISION
Derwent Class: P85; W02
International Patent Class (Additional): G09C-001/00; H04K-001/00; **H04L-009/00** ; H04N-007/16
File Segment: EPI; EngPI

30/5/48 (Item 42 from file: 350)
DIALOG(R)File 350:Derwent WPIX

004211305
WPI Acc No: 1985-038185/198506
XRPX Acc No: N85-028370
Scrambled television signal transmission - using three level key system with common second key for number of users giving short access time
Patent Assignee: INDEPENDENT BROADCASTING AUTH (INDE-N); MASON A G (MASO-I)
Inventor: MASON A G
Number of Countries: 012 Number of Patents: 012
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 8500491	A	19850131				198506	B
WO 8500718	A	19850214	WO 84GB236	A	19840702	198508	
EP 148235	A	19850717	EP 84902602	A	19840702	198529	
EP 151147	A	19850814	EP 84902601	A	19840702	198533	
JP 60501882	W	19851031				198550	
JP 60501883	W	19851031				198550	
EP 151147	B	19880420				198816	
US 4736422	A	19880405	US 85705422	A	19850222	198816	
DE 3470646	G	19880526				198822	
EP 148235	B	19881005				198840	
DE 3474496	G	19881110				198846	
US 4802215	A	19890131	US 85713904	A	19850315	198907	

Priority Applications (No Type Date): GB 8319817 A 19830722; GB 8317796 A 19830630
Cited Patents: EP 14654; US 4292650; WO 8301881; WO 8304154
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 8500491	A	E	25		
Designated States (National): JP US					
Designated States (Regional): AT BE CH DE FR GB LU NL SE					
WO 8500718	A	E			
Designated States (National): JP US					
Designated States (Regional): AT BE CH DE FR GB LU NL SE					
EP 148235	A	E			
Designated States (Regional): AT BE CH DE FR GB LI LU NL SE					
EP 151147	A	E			
Designated States (Regional): AT BE CH DE FR GB LI LU NL SE					
EP 151147	B	E			
Designated States (Regional): AT BE CH DE FR GB LI LU NL SE					
EP 148235	B	E			
Designated States (Regional): AT BE CH DE FR GB LI LU NL SE					

Abstract (Basic): WO 8500491 A

The information signal is scrambled and the scrambling technique used is identified. A number of identification signals (Tc) are generated, each representing information concerning a prospective user. A data block is produced by appending together a small number of information signals together with the encryptation key (P). The whole block is encrypted (1b) with a distribution key (D) common to the group of users. This reduces the time to cycle around all the subscribers in a given data capacity by reducing the total number of bits to be transmitted.

Apparatus receiving the scrambled signal has a decrypter (20) responsive to a user key signal (D). This recovers the key signal (P)

and the information relating to its receiver. A second decrypter (23) responds to this key signal to descramble the information signal (A).

USE/ADVANTAGE - Enables scrambled television signal to be descrambled by authorised viewers only. System is secure but time to access each user is short

1/4

Title Terms: SCRAMBLE; TELEVISION; SIGNAL; TRANSMISSION; THREE; LEVEL; KEY; SYSTEM; COMMON; SECOND; KEY; NUMBER; USER; SHORT; ACCESS; TIME
Derwent Class: W02
International Patent Class (Additional): H04K-001/00; **H04L-009/02** ; H04N-007/16
File Segment: EPI

30/5/49 (Item 43 from file: 350)
DIALOG(R)File 350:Derwent WPIX

003559251
WPI Acc No: 1983-A7440K/198303
XRPX Acc No: N83-009787

End-to-end encryption system - has network switch receiVing network-interchange request message and encrypted session key

Patent Assignee: VISA USA (VISA-N)
Inventor: ZEIDLER H M
Number of Countries: 003 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 68805	A	19830105	EP 82303266	A	19820623	198303	B
US 4423287	A	19831227	US 81278001	A	19810626	198403	
EP 68805	B	19861008				198641	
DE 3273666	G	19861113				198647	

Priority Applications (No Type Date): US 81278001 A 19810626
Cited Patents: EP 33833; EP 47285; GB 1517866; GB 2079504; US 4025760; US 4197986; US 4223403; US 4234932; US 4317957; WO 8002756; WO 8102655; EP 18129; EP 2389
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 68805	A	E	53		
Designated States (Regional): DE GB					
EP 68805	B	E			
Designated States (Regional): DE GB					

Abstract (Basic): EP 68805 A

A transaction terminal (10) transmits transaction information plus an encrypted PIN (personal identification number) to its associated acquirer station (12). The PIN being encrypted uses a session key, KSI, extracted at the terminal and decrypted using a first **master key** . The acquirer station sends on the message, with KSI encrypted in a second **master key** to a network switch which routes the message to the appropriate issuer station (20) with KSI re-encrypted in a third **master key** .

To avoid errors messages are pref. accompanied by authentication codes compared from it. The data processor at the issuer station verifies the transaction and returns an authorisation code (or denial code) via the switch (16) and acquirer station (12) to the originating terminal. The acquire station appends to the chain message a new session key KS2 encrypted using the first **master key** for use as the session key 11I in the next transaction.

Title Terms: END-TO-END; ENCRYPTION; SYSTEM; NETWORK; SWITCH; RECEIVE; NETWORK; INTERCHANGE; REQUEST; MESSAGE; ENCRYPTION; SESSION; KEY
Index Terms/Additional Words: AUTOMATIC; TELLER; MACHINE; CASH; DISPENSE
Derwent Class: T01; T05; W01
International Patent Class (Additional): **G06F-015/30** ; **H04L-009/00**
File Segment: EPI

```
Set     Items   Description
S1         77   AU=(TUNIMAN, D? OR TUNIMAN D? OR GOLDSCHMIDT, P? OR GOLDSC-
               HMIDT P? OR O'LEARY, M? OR O'LEARY M? OR KADYK, D? OR KADYK D-
               ?)
S2         30   S1 AND IC=H04L?
File 347:JAPIO Oct 1976-2003/Oct(Updated 040202)
         (c) 2004 JPO & JAPIO
File 348:EUROPEAN PATENTS 1978-2004/Feb W05
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040304,UT=20040226
         (c) 2004 WIPO/Univentio
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200416
         (c) 2004  THOMSON DERWENT
```

```
Set     Items   Description
S1        397   (ENCRYPT? OR ENCODE? OR CIPHER OR CIPHERS OR SECURITY)(2N)-
           (KEY OR KEYS)
S2      17676   FIRST OR 1ST OR PRIME OR PRIMARY OR INITIAL OR MAIN OR ORI-
           GINAL
S3      12441   SECOND OR 2ND OR ANOTHER OR ADDITIONAL
S4        695   (BASE OR SHARED OR PRIVATE OR LOCAL OR MASTER OR PUBLIC)(2-
           N)(KEY OR KEYS) OR PKI
S5        338   (DATA OR INFORMATION)()(STREAM? OR STRING? OR SEGMENT? OR -
           PIECE? OR PART? OR CHUNK? OR BLOCK?)
S6         92   (DATA OR INFORMATION)()(PART? OR SEGMENT? OR PORTION? OR P-
           IECE? OR MESSAGE()SPECIFIC OR SIGNATURE OR IDENTIF? OR ID)
S7        117   (HASH? OR KEY()SPLITTING OR CHECKSUM OR ONE()WAY()FUNCTION
           OR ALGORITHM?)(2N)(DATA OR INFORMATION OR DIGEST? OR FINGERPR-
           INT? OR FINGER()PRINT?)
S8          2   S1 AND S4 AND S5
S9          0   S1 AND S4 AND S6
S10         5   S1 AND S4 AND S7
S11         7   S8 OR S10
S12         7   S11 NOT PY>2001
S13         7   S12 NOT PD>20010107
File 256:SoftBase:Reviews,Companies&Prods. 82-2004/Feb
        (c)2004 Info.Sources Inc
```

13/5/1
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00125686 DOCUMENT TYPE: Review

PRODUCT NAMES: Internet Security (841944)

TITLE: Keys to the privacy-enabled enterprise
AUTHOR: Borck, James R
SOURCE: InfoWorld, v22 n37 p58(2) Sep 11, 2000
ISSN: 0199-6649
HOMEPAGE: http://www.infoworld.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Enterprises engaging in e-commerce gain the advantages of automated information exchange and reduced costs, but these activities create many new security exposures that must be addressed. Corporate data assets have to be protected in new ways when companies build alliances with external business associates. Because there are more access points to corporate **data streams** , a supply chain gateway can quickly become one of the weakest links in the privacy chain. Glitches and security holes are no long headed off at the perimeter of the internal network, but now can move into online venues of businesses and their trading partners. New trust mechanisms are required that are powerful and easy to use, and may include firewalls, hashing mechanisms, **encryption** , **public key** infrastructure (**PKI**), digital certificates, and extranet virtual private networks (VPNs). Hashing is based on a checksum process in which a sender delivers a message with an algorithm that allows the receiver to create a second hash upon receipt. Encryption protects text from prying eyes by converting it to unreadable characters; users encrypt and decrypt using unique keys. **PKI** allows distribution and management of **encryption keys** . Digital certificates authenticate users via digital 'fingerprints.' Extranet VPNs provide encryption, Pretty Good Privacy, **PKI** , and digital certificates to create a transmission path similar to that of a private leased line.

COMPANY NAME: Vendor Independent (999999)
SPECIAL FEATURE: Charts
DESCRIPTORS: Computer Security; Digital Certificates; E-Commerce; Encryption; Extranets; File Security; Firewalls; Internet Security; Network Administration; Network Software; System Monitoring
REVISION DATE: 20020630

13/5/2
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00118973 DOCUMENT TYPE: Review

PRODUCT NAMES: PKI **(838896**

TITLE: Public - key encryption
AUTHOR: Rothman, Mike
SOURCE: Network World, v16 n20 p35(1) May 17, 1999
ISSN: 0887-7661
HOMEPAGE: http://www.nwfusion.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Public Key Infrastructure (**PKI**) is becoming more popular as an identifier of users in e-commerce transactions. It also ensures that

documents have not been altered illegally during transmissi. **PKI** uses very long prime numbers, which are called keys. Two keys are used: a **private key** accessible only to the document's originator, and a **public key** , which is accessible to anyone. The two keys work in tandem, which means that a message scrambled with the **private key** can only be decoded with the **public key** ; the reverse is also true. The longer the string of digits in the keys, the more secure the process is. The user employs a digital signature to prove identity online, and **public key** cryptography makes sure that a document is run through a complex mathematical computation to output one large number, known as a **hash** . The original **data** and the **hash** cannot be separated, so that if either is changed, the hash does not match and the message cannot be decoded. Users can be sure that the correct key is available to verify the signature in a trusted system, which creates the need for a certificate authority to verify online identity. A certificate authority, which is like a digital passport bureau, is a trusted entity that makes **PKI** work. **Private keys** are securely generated, and after the sender's identity is verified, the certificate authority sings the sender's **public key** with a **private** root **key** . The combined **public key** and signature of the certificate authority complete the sender's digital certificate.

COMPANY NAME: Vendor Independent (999999)
SPECIAL FEATURE: Charts
DESCRIPTORS: Computer Security; E-Commerce; Encryption; File Security; File Transfer
REVISION DATE: 20000228

13/5/3
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00094883 DOCUMENT TYPE: Review

PRODUCT NAMES: OC://WebConnect Web 3270 Server for Java 1.2.2 Beta (632651)

TITLE: Access Internet, intranet with secure browser
AUTHOR: Staff
SOURCE: SunServer, v10 n8 p21(1) Aug 1996

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

OpenConnect Systems' OC://WebConnect Web 3270 Server for Java is a product in its 1.2.2 Beta release that allows secure access to corporate legacy data; the software allows authorized users anywhere on the globe to use a Java-enabled Web browser to gain access. An evaluation version makes encryption-secure Java **data stream** transfers between a Java-ready Web browser and an enterprise Web server over the public Internet or private intranets. OpenConnect President and CEO Stephen J. Clark says the software includes the widely used, industry-standard, powerful security technology of RSA Data Security. A licensing agreement extends RSA's encryption to Java applets to permit automated, unobtrusive exchange functions for encrypted data flows between end-users and the OC://WebConnect Server. The new release also uses the patented Diffie-Hellman **Public Key** Exchange for secure **encryption - key** management and industry standard data encryption; this technology provides the best commercially available security.

PRICE: $49

COMPANY NAME: OpenConnect Systems Inc (459186)
DESCRIPTORS: Computer Security; Data Communications; Encryption; File Transfer; Internet Security; Internetworking; Intranets; Java; Network Administration; Network Software

REVISION DATE: 20020630

13/5/4
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00090120 DOCUMENT TYPE: Review

PRODUCT NAMES: ViaCrypt PGP 4.0 Business Edition (532771)

TITLE: ViaCrypt key **to easy** security
AUTHOR: Peschel, Joe
SOURCE: InfoWorld, v18 n16 p121(1) Apr 15, 1996
ISSN: 0199-6649
HOMEPAGE: http://www.infoworld.com

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: A

ViaCrypt's ViaCrypt PGP (VPGP) Business Edition 4.0, a Windows electronic mail encryption package, provides the easiest to use interface for Pretty Good Privacy, the most popular encryption program available. Encryptor pastes encrypted text easily, and any task performed with free PGP's command line can be done using a mouse with VPGP. VPGP and freeware PGP both use **public key** cryptography, a method that creates a **public** and **private key** . PGP uses a secret key **algorithm** , International **Data** Encryption **Algorithm** (IDEA), to encrypt the body of a message, and RSA for encryption of the message key. ViaCrypt offers users a paid service for hard coding VPGP's options, corporate access, and certification keys. Laptop users can also temporarily carry overseas strong encryption tools without special paperwork.

PRICE: $149

COMPANY NAME: Network Associates Inc (613304)
SPECIAL FEATURE: Screen Layouts Charts
DESCRIPTORS: Computer Security; E-Mail Utilities; Encryption; File Security; IBM PC & Compatibles; Internet Security; Laptops; Mobile Computing; Network Software; Windows
REVISION DATE: 20020330

13/5/5
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00078703 DOCUMENT TYPE: Review

PRODUCT NAMES: Company--RSA Security Inc (860107)

TITLE: The Secret To Encryption
AUTHOR: Schatz, Willie
SOURCE: Information Week, v527 p74(2) May 15, 1995
ISSN: 8750-6874
HOMEPAGE: http://www.informationweek.com

RECORD TYPE: Review
REVIEW TYPE: Company

Electronic commerce is the driving force behind the data security movement. Encryption and authentication techniques are necessary to protect everything from electronic mail to financial transactions. RSA sells products based on a patented encryption algorithm developed in 1977. RSA's **Public Key** Cryptosystem uses two mathematical **keys** to **encrypt** and decrypt computer **data** . RSA's **algorithm** has been diligently tested and

was considered unbreakable until a 600-member team of Bell Communications Research scientists and mathematicians broke it last year. **Public Key** Cryptosystem's competitors include Cylink's Diffie-Hellman and MIT's Kerberos. A description of RSA's major clients and the way they use the system is included.

COMPANY NAME: RSA Security Inc (398047)
DESCRIPTORS: Computer Security; Encryption; Software Marketing
REVISION DATE: 20020703

13/5/6
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00078588 DOCUMENT TYPE: Review

PRODUCT NAMES: Pretty Good Privacy (835072)

TITLE: PGP: Pretty Good Privacy
AUTHOR: Collinson, Peter
SOURCE: SunExpert, v6 n6 p28(5) Jun 1995
ISSN: 1053-9239
HOMEPAGE: http://www.cpg.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

A UNIX consultant who sells software via the Internet, obtaining payment via credit card company connection, protects customer privacy with the Pretty Good Privacy (PGP) program, which secures e-mail via encryption. PGP uses the RSA Data **Security public key** algorithm for **encryption** , and the MD5 message **digest algorithm** for digital signatures. Keys are stored in 'keyrings' associated with user IDs; each PGP user must create **public** and **private keys** to which only UNIX superusers have unrestricted access. PGP also helps users establish trust in the e-mail system or in the World Wide Web. This is accomplished using a key 'fingerprint,' which generates the MD5 digest of a key on request. The program also allows keys to be signed, or certified as part and parcel of the ID in question. PGP can be obtained via anonymous FTP.

COMPANY NAME: Vendor Independent (999999)
DESCRIPTORS: Computer Security; E-Mail Utilities; Encryption; UNIX
REVISION DATE: 20000228

13/5/7
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00070303 DOCUMENT TYPE: Review

PRODUCT NAMES: ViaCrypt PGP Windows (532771)

TITLE: ViaCrypt PGP Brings 'Pretty Good Privacy' to Windows Systems
AUTHOR: Peschel, Joe
SOURCE: InfoWorld, v16 n44 p135(1) Oct 31, 1994
ISSN: 0199-6649
HOMEPAGE: http://www.infoworld.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

ViaCrypt PGP (Pretty Good Privacy) for Windows encrypts files using **public key** and conventional **encryption** methods. **Public key** methods use

the RSA algorithm, while conventional mode relies on International **Data** Encryption **Algorithm** (IDEA). The **public key** system uses two **keys**, **public** and secret to encrypt and decrypt files. When keys are used in combination with conventional mode, operations move along faster. The IDEA conventional mode can be used by itself, a viable method for encrypting plain, unencoded text. The user simply clicks the Key Management button to begin creating a set of **public** and private **keys**. Three **security** and speed selections are available, and speed is inversely proportional to data security. Management functions allow the user to handle several sets of keys, and the same menu allows keys to be copied, added, or removed.

COMPANY NAME: Network Associates Inc (613304)
DESCRIPTORS: Encryption; File Security; IBM PC & Compatibles; Windows
REVISION DATE: 20020321

```
Set     Items   Description
S1       4095   (ENCRYPT? OR ENCODE? OR CIPHER OR CIPHERS OR SECURITY)(2N)-
            (KEY OR KEYS)
S2    3892195   FIRST OR 1ST OR PRIME OR PRIMARY OR INITIAL OR MAIN OR ORI-
            GINAL
S3    1821453   SECOND OR 2ND OR ANOTHER OR ADDITIONAL
S4      12542   (BASE OR SHARED OR PRIVATE OR LOCAL OR MASTER OR PUBLIC)(2-
            N)(KEY OR KEYS) OR PKI
S5      16966   (DATA OR INFORMATION)()(STREAM? OR STRING? OR SEGMENT? OR -
            PIECE? OR PART? OR CHUNK? OR BLOCK?)
S6       7624   (DATA OR INFORMATION)()(PART? OR SEGMENT? OR PORTION? OR P-
            IECE? OR MESSAGE()SPECIFIC OR SIGNATURE OR IDENTIF? OR ID)
S7      45354   (HASH? OR KEY()SPLITTING OR CHECKSUM OR ONE()WAY()FUNCTION
            OR ALGORITHM?)(2N)(DATA OR INFORMATION OR DIGEST? OR FINGERPR-
            INT? OR FINGER()PRINT?)
S8         10   S2 (2W) S1
S9          8   S8 AND S4
S10       221   S2 (3N) S5
S11         0   S9 AND S10 AND S6
S12         0   S8 AND S10
S13         0   S9 AND S10
S14       134   S3 (2N) S5
S15         0   S14 AND S1
S16        14   S3 (2W) S1
S17        21   S8 OR S9 OR S16
S18        16   S17 NOT PY>2001
S19        16   S18 NOT PD>20010107
S20        14   RD (unique items)
File   8:Ei Compendex(R) 1970-2004/Feb W5
         (c) 2004 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2004/Feb
         (c) 2004 ProQuest Info&Learning
File 202:Info. Sci. & Tech. Abs. 1966-2004/Feb 27
         (c) 2004 EBSCO Publishing
File  65:Inside Conferences 1993-2004/Mar W1
         (c) 2004 BLDSC all rts. reserv.
File   2:INSPEC 1969-2004/Feb W5
         (c) 2004 Institution of Electrical Engineers
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File  94:JICST-EPlus 1985-2004/Feb W5
         (c)2004 Japan Science and Tech Corp(JST)
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Feb
         (c) 2004 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2004/Feb W4
         (c) 2004 FIZ TECHNIK
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
```

20/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

02889371 E.I. Monthly No: EI9004039865
Title: Intuition, perception, and secure communication.
Author: Arazi, Benjamin; Dinstein, Its'hak; Kafri, Oded
Corporate Source: Ben Gurion Univ, Dep of Electr & Comput Eng, Beer Sheva, Isr
Source: IEEE Transactions on Systems, Man and Cybernetics v 19 n 5 Sep-Oct 1989 p 1016-1020
Publication Year: 1989
CODEN: ISYMAW ISSN: 0018-9472
Language: English
Document Type: JA; (Journal Article) Treatment: A; (Applications); T; (Theoretical); X; (Experimental)
Journal Announcement: 9004
Abstract: The possibility of integrating human visual intelligence into the process of encrypting sensitive information by presenting certain visual information to the recipient's eye is discussed. This adds a new dimension to the cryptocomplexity of such a process. Two implementations that are based on this principle are described. The **first** shows how **keys** used for **encryption** can be randomly generated by the transmitter, without the necessity of exchanging them with the legitimate recipient. The keys are 'embedded' in a **master key** and are recovered from it by the intelligence of the legitimate recipient after he or she uses the **master key** . No human intelligence can be helpful to a user who does not possess the **master key** . The second implementation concerns the possibility of creating a secret connection between a numerical key and a specific image (e.g., a face). Such a scheme can be used, for example, in validating the identity of the users of credit cards. 5 Refs.
Descriptors: *CRYPTOGRAPHY; DATA PROCESSING--Security of Data
Identifiers: HUMAN VISUAL INTELLIGENCE; LINEAR ENCRIPTION TRANSFORMATION; RANDOMIZATION; CRYPTOCOMPLEXITY; CREDIT CARDS VALIDATION
Classification Codes:
723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

20/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

02574348 E.I. Monthly No: EI8805042793
Title: CRYPTOGRAPHICALLY SECURE PSEUDORANDOM SEQUENCE GENERATOR BASED ON RECIPROCAL NUMBER CRYPTOSYSTEM.
Author: Kurosawa, K.; Matsu, K.
Corporate Source: Tokyo Inst of Technology, Yokohama, Jpn
Source: Electronics Letters v 24 n 1 Jan 7 1988 p 16-17
Publication Year: 1988
CODEN: ELLEAK ISSN: 0013-5194
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 8805
Abstract: The letter presents a cryptographically secure pseudorandom sequence generator where two prime numbers are arbitrary, based on the **public key** cryptosystem proposed by one of the authors. (Author abstract) 3 refs.
Descriptors: *CRYPTOGRAPHY--*Reliability; DATA PROCESSING--Security of Data; INFORMATION THEORY
Identifiers: PSEUDORANDOM SEQUENCE GENERATOR; RECIPROCAL NUMBER; **PRIME** NUMBERS; **PUBLIC KEY** CRYPTOSYSTEM; CRYPTOGRAPHIC **SECURITY**
Classification Codes:
723 (Computer Software); 716 (Radar, Radio & TV Electronic Equipment); 717 (Electro-Optical Communications); 718 (Telephone & Line Communications)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS)

20/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

01138284 E.I. Monthly No: EI8208066354 E.I. Yearly No: EI82016402
Title: ON THE SECURITY OF MULTIPLE ENCRYPTION.
Author: Merkle, Ralph C.; Hellman, Martin E.
Corporate Source: Stanford Univ, Calif, USA
Source: Communications of the ACM v 24 n 7 Jul 1981 p 465-467
Publication Year: 1981
CODEN: CACMA2 ISSN: 0001-0782
Language: ENGLISH
Journal Announcement: 8208
Abstract: Double encryption has been suggested to strengthen the Federal Data Encryption Standard (DES). A recent proposal suggests that using two 56-bit keys but enciphering 3 times (encrypt with a first key, decrypt with a **second key**, then **encrypt** with the **first key** again) increases **security** over simple double encryption. It is shown that although either technique significantly improves security over single encryption, the new technique does not significantly increase security over simple double encryption. Cryptanalysis of the 112-bit key requires about 2**5**6 operations and words of memory, using a chosen plaintext attack. While DES is used as an example, the technique is applicable to any similar cipher. 13 refs.
Descriptors: *CODES, SYMBOLIC--*Encoding
Identifiers: CRYPTOGRAPHY
Classification Codes:
723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

20/5/4 (Item 4 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

00914770 E.I. Monthly No: EI8004027823 E.I. Yearly No: EI80015389
Title: UNIDIRECTIONAL CRYPTOGRAPHIC FUNCTIONS USING MASTER KEY VARIANTS.
Author: Lennon, R. E.; Matyas, S. M.
Corporate Source: IBM, Kingston, NY
Source: NTC Conf Rec Natl Telecommun Conf Washington, DC, Nov 27-29 1979. Publ by IEEE (Cat n 79CH1514-9), New York, NY 1979 v 3 p 43. 4. 1-43. 4. 5
Publication Year: 1979
CODEN: NTCCAM
Language: ENGLISH
Journal Announcement: 8004
Abstract: All cryptographic data systems require two basic operations -- encryption and decryption -- one being the inverse of the other. Effective key management operations which transform a key from " encipherment under one key to encipherment under **another key**, " using **encryption** and decryption operations, can negate the inverse properties of the two operations. There are two practical methods of implementing such a noninversion or unidirectional approach. One is to use different master keys for each transformation; another is to derive different keys from a single master key. An in depth analysis of the latter, more efficient approach is discussed. 6 refs.
Descriptors: *COMPUTER NETWORKS; COMPUTERS--Data Communication Systems
Identifiers: CRYPTOGRAPHY
Classification Codes:
723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

20/5/5 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

7179684 INSPEC Abstract Number: B2002-03-6120D-026, C2002-03-6130S-033
Title: Security tolerance and performance analysis of multi-keys KDC
Author(s): Zhang Xianggang; Liu Jinde
Author Affiliation: Coll. of Comput. Sci. & Eng., Univ. of Electron. Sci. & Technol. of China, Chengdu, China
Journal: Journal of University of Electronic Science and Technology of China vol.30, no.6 p.596-9
Publisher: Editorial Department of J. of UEST of China,
Publication Date: Dec. 2001 Country of Publication: China
CODEN: DKDAEM ISSN: 1001-0548
SICI: 1001-0548(200112)30:6L.596:STPA;1-Q
Material Identity Number: H166-2002-001
Language: Chinese Document Type: Journal Paper (JP)
Treatment: Practical (P); Theoretical (T)
Abstract: The keys management between users and the KDC (key distribution center) is changed to improve the security tolerance of the system and to alleviate the danger of a leaking key. Two methods are applied. In the **first**, different **key encryption keys** are applied between users and different KDC units, while, in the **second**, many **key encrypting keys** are applied for a data key before data communication to obtain the different parts of the data key. Results of a performance analysis are presented. (6 Refs)
Subfile: B C
Descriptors: **public key** cryptography; security of data
Identifiers: multi-keys KDC; security tolerance; performance analysis; keys management; key distribution center; encryption keys; data communication
Class Codes: B6120D (Cryptography); C6130S (Data security); C1260C (Cryptography theory)

20/5/6 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

7141015 INSPEC Abstract Number: B2002-02-1265F-021, C2002-02-5130-013
Title: Universal controller ties fate to emulation
Author(s): Morrison, D.
Author Affiliation: SoC designs, Livingston, UK
Journal: Integrated System Design vol.14, no.149 p.28-34
Publisher: CMP Media Inc,
Publication Date: Nov. 2001 Country of Publication: USA
CODEN: ISDNCY ISSN: 1080-2797
SICI: 1080-2797(200111)14:149L.28:UCTF;1-Z
Material Identity Number: F443-2001-014
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: System-on-chip (SoC) design service providers are under growing pressure to maximize flexibility in their designs and services. With the increased flexibility comes the need for more careful verification of the complete system. And emulation becomes central to verification. Clearly, when it comes to discussing SoC design, functional verification is one of the most highly charged subjects, and the Programmable Universal Controller device is no different. The SoC was aimed at the portable consumer appliances market, targeting such things as MP3 players and mobile phones. We spent a lot of time on feasibility studies trying to optimize requirements. A structured, well-planned functional verification approach accounted for 40 percent of the project's overall budget. As a result, the customer could process MP3 music on the device within a week of Tality's delivering initial samples. The device had several key requirements. First, as its name suggests, the Programmable Universal Controller had to be flexible to ensure it supported as many portable applications as possible. In addition, with the device targeted at portable applications, power consumption was a key consideration. This resulted in the implementation of several power-management modes and a powerful and extremely complex

clocking scheme. As with many such devices, data **security** is **another key** consideration and as a result, a great deal of time was spent to ensure that data stored in the embedded memory would be carefully partitioned and protected.
Subfile: B C
Descriptors: microcontrollers; programmable controllers
Identifiers: universal controller; emulation; functional verification; MP3 music; power consumption; data security; system-on-chip design
Class Codes: B1265F (Microprocessors and microcomputers); C5130 (Microprocessor chips); C3220B (Programmable controllers)

20/5/7 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

5410604 INSPEC Abstract Number: B9612-6120B-038, C9612-6130S-019
Title: Prime-number algorithm for public-key systems
Author(s): Kudin, A.M.
Journal: Kibernetika i Sistemnyi Analiz vol.31, no.6 p.112-20
Publisher: Plenum,
Publication Date: Nov.-Dec. 1995 Country of Publication: Ukraine
Material Identity Number: P784-96004
Translated in: Cybernetics and Systems Analysis vol.31, no.6 p.878-85
Publication Date: Nov.-Dec. 1995 Country of Publication: USA
CODEN: CYASEC ISSN: 1060-0396
SICI of Translation: 1060-0396(199511/12)31:6L.878:PNAP;1-Q
U.S. Copyright Clearance Center Code: 1060-0396/95/3106-0878$12.50
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P); Theoretical (T)
Abstract: We distinguish three distinct periods in the history of cryptography: until 1949, from 1949 to 1978, and since 1978 to the present. The beginning of the second period is marked by Shannon's paper "Theory of Communication in Secret Systems", presented at a closed seminar on communication theory in 1949. The "public key distribution" principle developed by Diffy and Hellnan in 1978 is usually viewed as marking the beginning of a new period in the history of cryptography, the period of cryptography with public (asymmetric) keys. Unlike the traditional symmetric encryption algorithms, in which the encrypting and decrypting keys are the same or can be easily obtained from one **another** , public- **key encryption** algorithms use different keys to encrypt and decrypt. These algorithms are therefore also known as asymmetric encryption algorithms. Full recognition of the advantages of public-key cryptosystems is evident in the publication of new international standards using asymmetric encryption algorithms. The RSA encryption algorithm is now a de facto standard for commercial software, and the USA National Institute of Standards and Technology has developed a draft Federal digital signature standard, which is based on El Gamal's encryption algorithm. The publication of standards has become possible despite the absence of a theoretical estimate of cryptosystem security. This is understandable, because such estimates are not available for the popular symmetric encryption algorithms either. (39 Refs)
Subfile: B C
Descriptors: computational complexity; public key cryptography
Identifiers: prime-number algorithm; public-key systems; cryptography; public-key encryption algorithms; international standards; cryptosystem security
Class Codes: B6120B (Codes); C6130S (Data security); C4240C (Computational complexity)

20/5/8 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

5408529 INSPEC Abstract Number: C9612-5620W-020
Title: Role of security technologies on the Internet
Author(s): Fujita, T.; Miyauchi, H.; Sako, K.; Masumoto, H.; Miyano, H.; Nakamura, K.
Journal: NEC Technical Journal vol.49, no.7 p.276-81
Publisher: NEC,
Publication Date: July 1996 Country of Publication: Japan
CODEN: NECGEZ ISSN: 0285-4139
SICI: 0285-4139(199607)49:7L.276:RSTI;1-O
Material Identity Number: H719-96011
Language: Japanese Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: This paper discusses some Internet security issues. At first, the NEC **original private - key encryption** algorithm ENCRiP is described, as well as the digital signature system IDSSS and key distribution system IDKDS. Then, the security middleware SIGURD is introduced together with its application to secure electronic mail and EDI systems. Finally, electronic voting is also introduced to clarify the importance of privacy enhanced systems on the Internet. (9 Refs)
Subfile: C
Descriptors: cryptography; Internet; security of data
Identifiers: Internet security issues; **private - key** encryption; ENCRiP; digital signature system; key distribution system; IDSSS; IDKDS; security middleware; SIGURD; secure electronic mail; EDI; electronic voting
Class Codes: C5620W (Other computer networks); C6130S (Data security)

20/5/9 (Item 5 from file: 2)
DIALOG(R)File 2:INSPEC

04309957 INSPEC Abstract Number: B9302-6150M-002, C9302-6130S-006
Title: Key management systems combining X9.17 and public key techniques
Author(s): Graff, J.
Author Affiliation: Cylink, Sunnyvale, CA, USA
Conference Title: 13th National Computer Security Conference. Proceedings. Information Systems Security. Standards - the Key to the Future p.49-61 vol.1
Publisher: NIST, Gaithersburg, MD, USA
Publication Date: 1990 Country of Publication: USA 2 vol. xi+839 pp.
Conference Sponsor: NIST
Conference Date: 1-4 Oct. 1990 Conference Location: Washington, DC, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: The paper describes a key management protocol that combines **public key** techniques with the symmetrical key techniques. The key management protocol standard for wholesale financial institutions, X9.17, serves as a basis for the proposed protocol. X9.17 uses manually delivered symmetric key encrypting keys to initially exchange keys. Subsequently, encryption keys, while encrypted under key encrypting keys, can be electronically transferred. The Cylink CIDEC-LS link encryptor's key management system serves as a basis for a practical, initial model of incorporating **public key** techniques as a supplement to X9.17. The protocol permits the establishment of **initial key encrypting keys** using the Diffie-Hellman **public key** algorithm. The paper then discusses the further enhancements to achieve a key management system suitable for a dynamic network such as a local area network (LAN). A recently proposed companion standard to X9.17 and a suggested method for key management to IEEE 802.10, SILS, have been developed from the concepts presented. Additionally, the paper discusses the various properties of the available **public key** algorithms. (11 Refs)
Subfile: B C
Descriptors: protocols; **public key** cryptography
Identifiers: X9.17; **public key** techniques; key management protocol;

symmetrical key techniques; wholesale financial institutions; symmetric key encrypting keys; Cylink CIDEC-LS link; Diffie-Hellman **public key** algorithm; dynamic network; local area network; IEEE 802.10; SILS
Class Codes: B6150M (Protocols); B6120B (Codes); C6130S (Data security); C5640 (Protocols)

20/5/10 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC

03071718 INSPEC Abstract Number: B88015281, D88000730
Title: Key telephone systems: hybrid units add PB X-like features
Author(s): Axner, D.H.
Author Affiliation: Management Information Corp., Cherry Hill, NJ, USA
Journal: Telecommunication Products Plus Technology vol.5, no.11 p. 56-8, 60, 62, 64
Publication Date: Nov. 1987 Country of Publication: USA
CODEN: TPPTEA ISSN: 0746-6072
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: Modern key systems distribute processing power throughout the telephone network, and use switching matrices to interconnect stations and lines. The growing trend in technology is away from space-division switching-an older analog technique-to more useful digital switching using TDM (time-division multiplexing) and PAM- or PCM- **encoded** signals. **Another key** facet of modern key system technology is the ability to program the features and restrictions on multi-button keysets, providing even greater operating flexibility for users. They can configure an entire system, restricting features and access to long-distance lines on some telephones and providing expanding features with unlimited toll access on others. The growing trend in the industry is toward programmable buttons ('soft keys') on telephone keysets that can be assigned added lines ('line appearances') and/or other features. (0 Refs)
Subfile: B D
Descriptors: electronic switching systems; private telephone exchanges
Identifiers: PBX; hybrid units; distributed processing; key telephone systems; switching matrices; digital switching; time-division multiplexing; multi-button keysets; programmable buttons; soft keys; line appearances
Class Codes: B6210D (Telephony); B6230B (Electronic telephone exchanges); D4070 (Telephone systems)

20/5/11 (Item 7 from file: 2)
DIALOG(R)File 2:INSPEC

02980328 INSPEC Abstract Number: C87056740
Title: How to evaluate microcomputer encryption software and hardware
Author(s): Highland, H.J.
Author Affiliation: CompuLit Inc., Elmont, NY, USA
Journal: Computers & Security vol.6, no.3 p.229-44
Publication Date: June 1987 Country of Publication: Netherlands
CODEN: CPSEDU ISSN: 0167-4048
U.S. Copyright Clearance Center Code: 0167-4048/87/$3.50
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: Most companies are not equipped to make exhaustive comparisons of the encryption software and hardware products available in the market today. It is often difficult to make a sensible choice because full information is not found in the product's promotional literature and there are no definitive guidelines available to assist the user in making a selection. This paper presents a number of factors to be evaluated prior to making a selection. The author starts with basic question to consider before a search begins. Then he discusses the need for a controlled environment in which to evaluate encryption products and what this environment should be. Then comes the evaluation of encryption features

followed by encryption timing and file size consideration. **Additional** attributes of **encryption** packages including **key** characteristics and file recovery are discussed. Finally test procedures are considered. (0 Refs)
Subfile: C
Descriptors: cryptography; equipment selection (computers); microcomputer applications; software selection
Identifiers: security of data; DES; encryption product evaluation; testing; checklists; microcomputer encryption software; guidelines; encryption features; encryption timing; file size; encryption packages; file recovery
Class Codes: C0310H (Equipment and software evaluation methods); C6130 (Data handling techniques)

20/5/12 (Item 8 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

01357734 INSPEC Abstract Number: B79026386, C79015784
Title: Expand a keyboard matrix by adding isolation diodes to a key encoder
Author(s): Buurma, G.; Caseldine, J.
Author Affiliation: Nat. Semiconductor, Santa Clara, CA, USA
Journal: Electronic Design vol.26, no.25 p.120
Publication Date: 6 Dec. 1978 Country of Publication: USA
CODEN: ELODAW ISSN: 0013-4872
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: Add a **second** matrix of **keys** to an **encoded** keyboard matrix by using four isolation diodes and a NAND gate. The 74C922 CMOS key encoder scans, detects, debounces, encodes and latches the key positions in an array of single-pole, single-throw keys. (0 Refs)
Subfile: B C
Descriptors: field effect integrated circuits; integrated logic circuits; keyboards
Identifiers: keyboard matrix; key encoder; CMOS key encoder; NAND gate; flip flops; three state buffer; four input gate; four row capability
Class Codes: B1265B (Logic circuits); B2570D (CMOS integrated circuits); C5120 (Logic and switching circuits); C5500 (Computer peripheral equipment)

20/5/13 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus
(c)2004 Japan Science and Tech Corp(JST). All rts. reserv.

04336654 JICST ACCESSION NUMBER: 99A0708336 FILE SEGMENT: JICST-E
Information Security. Development of Cryptography and Key Recovery System.
SHIMBO ATSUSHI (1); SANO FUMIHIKO (1); NIWA AKITO (1)
(1) Toshiba Corp.
Toshiba Rebyu(Toshiba Review), 1999, VOL.54,NO.7, PAGE.8-11, FIG.4, REF.4
JOURNAL NUMBER: F0360AAK ISSN NO: 0372-0462 CODEN: TORBA
UNIVERSAL DECIMAL CLASSIFICATION: 621.391.037.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: Safer encryption algorithms and signature schemes have been actively resarched in recent years. Candidates for the advanced encryption standard(AES), which use a key length exceeding 128 bits, and the elliptic curve cryptosystem are prominent in the fields of symmetric- **key** cryptography and **public** - **key** cryptography, respectively. Toshiba has developed **original** symmetric- **key** block **ciphers** that are safer than Data Encryption Standard(DES) or triple-DES, as well as a fast algorithm for computing in the elliptic curve cryptosystem, and has applied these results to the development of

a key recovery system. In this system, an encrypted message is decryptable under agreement by approvers, even if the decryption key is lost at lawful nodes. (author abst.)
DESCRIPTORS: computer security; cryptogram; **public key** cryptography; cryptography key; algorithm; safety analysis; ellipse; number theory; decoding; Galois field; operation(mathematics
IDENTIFIERS: information security; secret key cryptosystem
BROADER DESCRIPTORS: security; guarantee; analysis; circle; conic section; curve; line; mathematics; modification; signal processing; treatment; field(mathematics); algebraic system
CLASSIFICATION CODE(S): ND02030R

20/5/14 (Item 2 from file: 94)
DIALOG(R)File 94:JICST-EPlus

03000563 JICST ACCESSION NUMBER: 96A0808945 FILE SEGMENT: JICST-E
Internet. Role of Security Technologies on the Internet.
FUJITA TOMOYUKI (1); MIYAUCHI HIROSHI (1); SAKO KAZUE (1); MASUMOTO HIROYUKI (1); NAKAMURA KATSUHIRO (1); MIYANO HIROSHI (2)
(1) NEC Corp.; (2) Telecommunication Satellite Corp. of Japan
NEC Giho(NEC Technical Journal), 1996, VOL.49,NO.7, PAGE.276-281, FIG.6, REF.9
JOURNAL NUMBER: G0475BAB ISSN NO: 0285-4139
UNIVERSAL DECIMAL CLASSIFICATION: 681.3:654 681.3.02-759
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: This paper discusses some Internet security issues. At first, the NEC **original private - key encryption** algorithm ENCRiP is described, as well as the digital signature system IDSSS and key distribution system IDKDS. Then, the security middleware SIGURD is introduced together with its application to secure electronic mail and EDI systems. Finally, electronic voting is also introduced to clarify the importance of privacy enhanced systems on the Internet. (author abst.)
DESCRIPTORS: computer network; computer security; cryptogram; **public key** cryptography; digital signature; privacy; data protection; multi-media ; protocol; database; interconnection; interface; internet; cryptography key; middleware; electronic mail
BROADER DESCRIPTORS: communication network; information network; network; security; guarantee; right; protection; information media; rule; connection; system program; computer program; software; telecommunication
CLASSIFICATION CODE(S): JC03000K; JD01020V

```
Set     Items   Description
S1      27884   (ENCRYPT? OR ENCODE? OR CIPHER OR CIPHERS OR SECURITY)(2N)-
             (KEY OR KEYS)
S2    9341809   FIRST OR 1ST OR PRIME OR PRIMARY OR INITIAL OR MAIN OR ORI-
             GINAL
S3    6963614   SECOND OR 2ND OR ANOTHER OR ADDITIONAL
S4      55192   (BASE OR SHARED OR PRIVATE OR LOCAL OR MASTER OR PUBLIC)(2-
             N)(KEY OR KEYS) OR PKI
S5      37853   (DATA OR INFORMATION)()(STREAM? OR STRING? OR SEGMENT? OR -
             PIECE? OR PART? OR CHUNK? OR BLOCK?)
S6      15861   (DATA OR INFORMATION)()(PART? OR SEGMENT? OR PORTION? OR P-
             IECE? OR MESSAGE()SPECIFIC OR SIGNATURE OR IDENTIF? OR ID)
S7       8744   (HASH? OR KEY()SPLITTING OR CHECKSUM OR ONE()WAY()FUNCTION
             OR ALGORITHM?)(2N)(DATA OR INFORMATION OR DIGEST? OR FINGERPR-
             INT? OR FINGER()PRINT?)
S8        133   S2 (2W) S1
S9         51   S8 (S) S4
S10       531   S2 (3N) S5
S11         0   S9 (S) S10 (S) S6
S12         0   S8 (S) S10
S13         0   S9 (S) S10
S14       717   S3 (3N) S5
S15       403   S3 (3N) S1
S16         0   S8 AND S9 AND S10 AND S14 AND S15
S17         0   S9 (S) S10
S18         0   S9 (S) S14
S19         1   S9 (S) S15
S20         2   S14 (S) S1
S21       229   S3 (2W) S1
S22       404   S2 (2N) S5
S23       404   S10 (S) S22
S24       133   S23 (S) S6
S25         0   S24 (S) S7
S26       133   S24 (S) S5
S27         1   S14 (S) S15
S28       186   S9 OR S19 OR S20 OR S26 OR S27
S29        24   S28 AND ((MOBILE OR PORTABLE OR CELLULAR OR CELL OR WIRELE-
             SS)(2W)(DEVICE? OR CLIENT? OR NODE? OR TELECOMMUNICATION? OR -
             COMPUTER? OR PHONE? OR TELEPHONE? OR TERMINAL) OR CELLPHONE? -
             OR CELL()PHONE? OR WIRELESS OR WIRE()LESS OR RADIO?)
S30         9   S29 NOT PY>1998
S31         7   S30 NOT PD>19980107
S32         5   RD (unique items)
File  15:ABI/Inform(R) 1971-2004/Mar 10
         (c) 2004 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 647:CMP  Computer Fulltext 1988-2004/Feb W5
         (c) 2004 CMP Media, LLC
File 275:Gale Group Computer DB(TM) 1983-2004/Mar 10
         (c) 2004 The Gale Group
File 674:Computer News Fulltext 1989-2004/Feb W5
         (c) 2004 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2004/Mar 09
         (c) 2004 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2004/Mar 09
         (c) 2004 McGraw-Hill Co. Inc
File 636:Gale Group Newsletter DB(TM) 1987-2004/Mar 10
         (c) 2004 The Gale Group
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2004/Mar 10
         (c) 2004 PR Newswire Association Inc
File  16:Gale Group PROMT(R) 1990-2004/Mar 10
         (c) 2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
```

32/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00691891 93-41112
To tap or not to tap
Denning, Dorothy E
Communications of the ACM v36n3 PP: 24-33 Mar 1993
ISSN: 0001-0782 JRNL CODE: ACM
WORD COUNT: 6959

...TEXT: and services such as ISDN (Integrated Services digital Network), fiber optic transmissions, and the increasing number of **mobile telecommunication** networks and architectures. Although it is technically feasible to intercept digital communications, not all systems have been... the trustee. For example, two trustees could be used, and the keys could be stored with the **first** trustee **encrypted** under a **key** known only to the second. Alternatively, using Silvio Micali's "fair **public - key** cryptography," each user's **private key** could be split into, say, five pieces, and each piece given to a different trustee 4!. The...

32/3,K/2 (Item 1 from file: 810)
DIALOG(R)File 810:Business Wire

0614457 BW0258

Business Wire Recap

August 14, 1996

Byline: Editors

...Solutions Limited appoints three new vice presidents; worldwide sales & marketing activities increase for (BW1040 08:00)
(WESTERN- **WIRELESS**)(WWCA) ISSAQUAH, Wash.--Western **Wireless** continues its rapid growth with launch of Portland, Oregon, PCS System; Newest market represents company's fourth...Rochester, New York; Telecasts New York v. Ortiz Live (BW1193 10:56)
(FIRST-DATA)(FDC) OMAHA, Neb.-- **First Data Partners** with National City to Provide Processing and Information Management Services (BW0067 10:57)
(EXECUTONE)(XTON) MILFORD, Conn...

32/3,K/3 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01937755 SUPPLIER NUMBER: 18280554 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Surfing the yellow pages. (interactive on-line telephone books) (Industry Trend or Event)
Mehta, Suketu
LAN Magazine, v11, n6, p77(7)
June, 1996
ISSN: 1069-5621 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 5844 LINE COUNT: 00470

...ABSTRACT: in its infancy. However, advertising on the Internet promises to eventually edge out printed directories as the **primary** source of **information** , **particularly** for users considering major purchases. Electronic directories offer greater scope and depth of information and the information...
... well into the foreseeable future. In recent history, a new medium rarely pushes out another medium entirely: **Radio** did not do away with newspapers, television did not do away with **radio** , and electronic on-line

services will not preclude paper-based directories. The challenge, then, is to develop...limited by the Internet. It's unlikely, but the Internet could turn out to be the CB **radio** of the 1990s.

32/3,K/4 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01890577 SUPPLIER NUMBER: 17826195 (USE FORMAT 7 OR 9 FOR FULL TEXT)
These are the headlines and first paragraphs of each story, in order:.
Newsbytes, pNEW01220033
Jan 22, 1996
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1264 LINE COUNT: 00128

TEXT:
...5-Inch Disk Drive -- Fisher International Systems of Naples, Florida, has introduced Crypto SmartDisk, calling it the " **first public key encryption** technology on a standard 3.5-inch disk." The new technology allows any user with a standard...
... mail the company.
10) Netherlands - GSM Take-Up Exceeds Expectations -- Libertel, the second GSM (global system for **mobile** communications) digital **phone** network in the Netherlands, has revealed that it has signed more than 27,000 subscribers up in...president and chief executive officer, has resigned. However, in the meantime, the company has rolled out new **radio** frequency identification products.
29) Compton's Has No Comment On Shutdown -- Neither Softkey International nor Compton's...

32/3,K/5 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01591704 SUPPLIER NUMBER: 13643287 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Dorothy E. Denning. (To Tap or Not to Tap)
Denning, Dorothy E.
Communications of the ACM, v36, n3, p26(8)
March, 1993
ISSN: 0001-0782 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 7105 LINE COUNT: 00589

... and services such as ISDN (Integrated Services Digital Network), fiber optic transmissions, and the increasing number of **mobile telecommunication** networks and architectures. Although it is technically feasible to intercept digital communications, not all systems have been... the trustee. For example, two trustees could be used, and the keys could be stored with the **first** trustee **encrypted** under a **key** known only to the second. Alternatively, using Silvio Micali's "fair **public** - **key** cryptography," each user's **private key** could be split into, say, five pieces, and each piece given to a different trustee [4]. The...